Chapter 12
Secure Communications and Network Attacks

THE CISSP TOPICS COVERED IN THIS CHAPTER INCLUDE:

- ✓ **Domain 4.0: Communication and Network Security**
  - 4.1 Apply secure design principles in network architectures
    - 4.1.7 Performance metrics (e.g., bandwidth, latency, jitter, throughput, signal-to-noise ratio)
    - 4.1.18 Monitoring and management (e.g., network observability, traffic flow/shaping, capacity management, fault detection and handling)
  - 4.3 Implement secure communication channels according to design
    - 4.3.1 Voice, video, and collaboration (e.g., conferencing, Zoom rooms)
    - 4.3.2 Remote access (e.g., network administrative functions)
    - 4.3.3 Data communications (e.g., backhaul networks, satellite)
    - 4.3.4 Third-party connectivity (e.g., telecom providers, hardware support)

Communications security is designed to detect, prevent, and even correct data transportation errors (that is, it provides integrity protection as well as confidentiality). Communications security is used to sustain the security of networks while supporting the need to

exchange and share data. This chapter covers the many forms of communications security, vulnerabilities, and countermeasures.

The Communication and Network Security domain deals with topics related to network components (i.e., network devices and protocols), specifically how they function and how they are relevant to security. This domain is discussed in this chapter and in Chapter 11, "Secure Network Architecture and Components." Be sure to read and study the material in both chapters to ensure complete coverage of the essential material.

Protocol Security Mechanisms

Transmission Control Protocol/Internet Protocol (TCP/IP) is the primary protocol suite used on most networks and on the Internet. It is a robust protocol suite, but it has numerous security deficiencies. In an effort to improve the security of TCP/IP, many subprotocols, mechanisms, or applications have been developed to protect the confidentiality, integrity, and availability of transmitted data. It is important to remember that even with the foundational protocol suite of TCP/IP, there are literally hundreds, if not thousands, of individual protocols, mechanisms, and applications in use across the Internet. Some of them are designed to provide security services. Some protect integrity, others protect confidentiality, and others provide authentication and access control. In the next sections, we'll discuss some common network and protocol security mechanisms.

Authentication Protocols

The *Point-to-Point Protocol (PPP)* is an encapsulation protocol designed to support the transmission of IP traffic over dial-up or point-to-point links. PPP is a Data Link Layer protocol that allows for multivendor interoperability of WAN devices supporting serial links. Although it is rarely found on typical Ethernet networks today, it is the foundation on which many modern communications are based, as well as the foundation of communication authentication. PPP includes a wide range of communication services, such as the assignment and management of IP addresses, management of synchronous communications, standardized encapsulation,

multiplexing, link configuration, link quality testing, error detection, and feature or option negotiation (such as compression).

PPP is an Internet standard documented in RFC 1661. It replaced the *Serial Line Internet Protocol (SLIP)*. SLIP offered no authentication, supported only half-duplex communications, had no error-detection capabilities, and required manual link establishment and teardown. PPP supports automatic connection configuration, error detection, full-duplex communications, and options for authentication. The original PPP options for authentication were PAP, CHAP, and EAP.

Password Authentication Protocol (PAP) PAP transmits usernames and passwords in cleartext. It offers no form of encryption; it simply provides a means to transport the logon credentials from the client to the authentication server.

Challenge Handshake Authentication Protocol (CHAP) CHAP performs authentication using a challenge-response dialogue that cannot be replayed. A challenge is a random number issued by the server, which the client uses along with the password hash to compute the one-way function-derived response. CHAP also periodically reauthenticates the remote system throughout an established communication session to verify the persistent identity of the remote client. This activity is transparent to the user. However, since CHAP is based on MD5, it is no longer considered secure. A Microsoft customization named MS-CHAPv2 uses updated algorithms, adds optional session encryption, and is preferred over the original CHAP.

Extensible Authentication Protocol (EAP) This is a framework for authentication instead of an actual protocol. EAP allows customized authentication security solutions, such as supporting smartcards, tokens, and biometrics. EAP was originally designed for use over physically isolated channels and thus assumed secured pathways. Some EAP methods use encryption, but others do not. Over 40 EAP methods are defined, including LEAP, PEAP, EAP-SIM, EAP-FAST, EAP-MD5, EAP-POTP, EAP-TLS, and EAP-TTLS.

EAP Derivatives

Lightweight Extensible Authentication Protocol (LEAP) is a Cisco proprietary alternative to TKIP for WPA. It was developed to address deficiencies in TKIP before 802.11i/WPA2 was ratified as a standard. LEAP is now a legacy solution to be avoided.

Protected Extensible Authentication Protocol (PEAP) encapsulates EAP in a TLS tunnel. PEAP is preferred to EAP because PEAP imposes its own security. PEAP supports mutual authentication.

Subscriber Identity Module (EAP-SIM) is a means of authenticating mobile devices over the Global System for Mobile Communications (GSM) network. Each device/subscriber is issued a subscriber identity module (SIM) card, which is associated with the subscriber's account and service level.

Flexible Authentication via Secure Tunneling (EAP-FAST) is a Cisco protocol proposed to replace LEAP, which is now obsolete, thanks to the development of WPA2.

EAP-MD5 was one of the earliest EAP methods. It hashes passwords using MD5. It is now deprecated.

EAP Protected One-Time Password (EAP-POTP) supports the use of OTP tokens (which includes hardware devices and software solutions) in multifactor authentication for use in both one-way and mutual authentication.

EAP Transport Layer Security (EAP-TLS) is an open IETF standard that implements the TLS protocol for use in protecting authentication traffic. EAP-TLS is most effective when both client and server have a digital certificate (i.e., mutual certificate authentication).

EAP Tunneled Transport Layer Security (EAP-TTLS) is an extension of EAP-TLS that creates a VPN-like tunnel between endpoints prior to authentication. This ensures that even the client's username is never transmitted in cleartext.

EAP Internet Key Exchange v. 2 (EAP-IKEv2) is based on the IKEv2 (Internet Key Exchange) protocol from IPSec. It provides mutual authentication, session key establishment, and supports authentication using passwords, symmetric keys, or asymmetric key pairs.

Nimble out-of-band authentication for EAP (EAP-NOOB) is a versatile bootstrapping solution for devices lacking preconfigured authentication credentials and those not yet registered on any server. It uses various OOB channels, such as QR codes, NFC tags, and audio. It is particularly useful for Internet-of-Things (IoT) gadgets and toys that arrive without any details regarding ownership, network affiliation, or server registration. For a more extensive list of EAP methods, see http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol.

IEEE 802.1X defines the use of encapsulated EAP to support a wide range of authentication options for LAN connections. The *IEEE 802.1X* standard is formally named "Port-Based Network Access Control," where *port* refers to any network link, not just physical RJ-45 jacks. This technology ensures that clients can't communicate with a resource until proper authentication has taken place. It's based on Extensible Authentication Protocol (EAP) from PPP.

Many people encounter 802.1X in relation to wireless networking, where it serves as the basis for wireless enterprise authentication. In that implementation, 802.1X serves as an authentication proxy by forwarding wireless client authentication requests to a dedicated remote authentication server or AAA server (typically RADIUS or TACACS+; see Chapter 14, "Controlling and Monitoring Access").

Thus, it is important to remember that 802.1X isn't a wireless technology (i.e., IEEE 802.11)—it is an authentication technology that can be used anywhere authentication is needed, including WAPs, firewalls, routers, switches, proxies, VPN gateways, and remote access servers (RASs)/network access servers (NASs).

When 802.1X is in use, it makes a port-based decision about whether to allow or deny a connection based on the authentication of a user or service.

Like many technologies, 802.1X may be vulnerable to adversary-in-the-middle (AiTM) (aka MiTM or on-path) and hijacking attacks because the authentication mechanism occurs only when the connection is established. Not all 802.1X or EAP authentication methods are secure; some only check for superficial IDs, such as a MAC address, before granting access. This issue can be addressed by using periodic mid-session reauthentication, as well as implementing session encryption in addition to any authentication protections provided by 802.1X/EAP.

For a discussion of 802.1X, LEAP, and PEAP in relation to wireless networking, see Chapter 11, “Secure Network Architecture and Components.”

Port Security

Port security in IT can mean several things. It can mean the physical control of all connection points, such as RJ-45 wall jacks or device ports (such as those on a switch, router, or patch panel), so that no unauthorized users or devices can attempt to connect to an open port. This control can be accomplished by locking down the wiring closet and server vaults and then disconnecting the workstation run from the patch panel (or punch-down block) that leads to a room's wall jack. Any unneeded or unused wall jacks can (and should) be physically disabled in this manner. Another option is to use a smart patch panel that can monitor the MAC address of any device connected to each wall port across a building and detect not just when a new device is connected to an empty port, but also when a valid device is disconnected or replaced by an invalid device.

Another meaning for port security is the management of TCP and User Datagram Protocol (UDP) ports. If a service is active and assigned to a port, then that port is open. All the other 65,535 ports (TCP or UDP) are closed if a service isn't actively using them. Threat actors can detect the presence of active services by performing a port scan. Firewalls, IDSs, IPSs, and other security tools can detect this activity and either block it or send back false/misleading information. This measure is a type of port security that makes port scanning less effective.

Port security can also refer to the need to authenticate to a port before being allowed to communicate through or across the port. This may be implemented on a switch, router, smart patch panel, or even a wireless network. This concept is often referred to as IEEE 802.1X. For the full discussion of network access control (NAC), see Chapter 11.

Quality of Service (QoS)

Quality of service (QoS) is the oversight and management of the efficiency and performance of network communications. QoS controls protect the availability of data networks under load. Many different factors contribute to the quality of the end-user experience, and QoS attempts to manage all of those factors to create an experience that meets business requirements.

Some of the performance metrics or factors contributing to QoS are as follows:

Bandwidth The network capacity available to carry communications.

Latency The time it takes a packet to travel from source to destination.

Jitter The variation in latency between different packets.

Packet Loss Some packets may be lost between source and destination, requiring retransmission.

Interference Electrical noise, faulty equipment, and other factors may corrupt the contents of packets.

Throughput The actual amount of data transmitted successfully over a network or communication channel within a given period. It is a measure of the effective data transfer rate and represents the real-world performance of the network.

Signal-to-Noise Ratio (SNR) A measure of the quality of a signal in a communication channel. It compares the strength of the desired signal to the level of background noise or interference present in the channel. The higher the SNR, the better the quality of the signal.

Based on the recorded/detected metrics in these areas, network traffic can be adjusted, throttled, or reshaped to account for unwanted conditions. QoS systems often prioritize certain traffic types that have a low tolerance for interference and/or have high business requirements. High-priority traffic or time-sensitive traffic (such as VoIP) can be prioritized, and other traffic can be held back as needed. Throttling or shaping can be implemented on a protocol or IP basis to set a maximum use or consumption limit. In some cases, using alternate transmission paths, time-shifting noncritical data transfers, or deploying more or higher-capacity connections may be necessary to maintain a desired QoS.

Most network administrators don't automatically consider QoS an aspect of security. However, availability is one of the elements of the CIA Triad. By monitoring and managing QoS, essential communications and their related business operations, processes, and tasks may have their availability sustained and protected. QoS may also include specific security requirements, such as requiring encryption for certain types of traffic.

Transparency is the characteristic of a service, security control, or access mechanism that ensures that it is unseen by users. The more transparent a security mechanism is, the less likely a user will be able to circumvent it or even be aware that it exists. With transparency, there is a lack of direct evidence that a feature, service, or restriction exists, and its impact on performance is minimal.

Secure Voice Communications

Telephony is the collection of methods by which telephone services are provided to an organization or the mechanisms by which an organization uses telephone services for either voice and/or data communications. Telephony includes *public switched telephone network (PSTN)* (aka plain old telephone service, or POTS), private branch exchange (PBX), mobile/cellular services (see Chapter 9,

“Security Vulnerabilities, Threats, and Countermeasures”), and VoIP.

Public Switched Telephone Network

The vulnerability of voice communication is tangentially related to IT system security. However, most voice communication solutions have moved on to the network (i.e., technology convergence) by employing digital devices and VoIP; therefore, securing voice communications is an increasingly important issue. When voice communications occur over the IT infrastructure, it is important to implement mechanisms to provide for authentication and integrity. Confidentiality should be maintained by employing an encryption service or protocol to protect voice communications while in transit.

PBX and PSTN voice communications are vulnerable to interception, eavesdropping, tapping, and other exploitations. Often, physical security is required to maintain control over voice communications within the confines of your organization's physical locations. Security of voice communications outside your organization is typically the responsibility of the phone company from which you lease services. If voice communication vulnerabilities are an important issue for sustaining your security policy, you should deploy an encrypted communication mechanism and use it exclusively.

PSTN connections were the only or primary remote network links for many businesses until high-speed, cost-effective, and ubiquitous access methods were available. POTS/PSTN also waned in use for home-user Internet connectivity once broadband and wireless services became more widely available. However, PSTN connections are sometimes still used as a backup option for remote connections when broadband solutions fail. PSTN may still be the only option for rural Internet and remote connections. PSTN is also used as standard voice lines when VoIP or broadband solutions are unavailable, interrupted, or not cost-effective.

Voice over Internet Protocol (VoIP)

Voice over Internet Protocol (VoIP) is a technology that encapsulates audio into IP packets to support telephone calls over TCP/IP network connections. VoIP is also the basis for many multimedia

messaging services that combine audio, video, chat, file exchange, whiteboard, and application collaboration.

In Chapter 11, we discussed VoIP and mentioned that Secure Real-time Transport Protocol (SRTP) may be used to provide encryption. However, it is important to clarify when and if this encryption is of any use. VoIP encryption is widely available but rarely end-to-end. VoIP is not a single technology, even though it uses common standardized protocols—just as there are many different operating systems that communicate over the TCP/IP protocol suite. VoIP products from different vendors often do not interoperate on anything other than the transmission of the audio communication itself.

For example, if you have VoIP phone service provided by your ISP, you may have a VoIP phone sitting on your desk that looks and acts like a traditional PSTN phone. The difference is that it is plugged into the LAN rather than a telephone line. The VoIP service provided by your ISP might not offer any form of encryption. Thus, it would be impossible to obtain end-to-end encryption using that service. However, even if your ISP provided encrypted VoIP services, it would only establish end-to-end encryption if you called someone using the same ISP-provided VoIP service. If you called someone using another VoIP solution, you likely would not end up with an end-to-end encrypted connection.

This is one of the most misunderstood aspects of VoIP services. It is often marketed as being an encrypted service. However, the advertisements fail to point out that the encryption is only established between compatible devices and service providers, which is usually limited to their own proprietary variation of VoIP. In order to communicate with another phone outside of the ISP's VoIP services, a VoIP-to-PSTN gateway must be present. This gateway supports calls from a VoIP phone to make their way to a traditional PSTN landline or mobile phone, and vice versa. If you are using ISP A's VoIP service to call someone using ISP B's VoIP service, your call will likely go through one or more gateways and likely traverse some portion of the PSTN network. Therefore, your call may be encrypted from your phone to the gateway, but it will have to be decrypted to traverse the gateway and the intermediary network. When the

connection reaches the callee's service gateway, it may be encrypted again from the gateway to the destination phone.

There are likely some VoIP providers that have a direct gateway interface between their VoIP solution and another VoIP provider's network, but unless they happen to have compatible configurations, they still will have to decrypt and re-encrypt at the gateway. Therefore, unless you stay within the same VoIP provider's network, you cannot be assured that your connection is protected by end-to-end encryption.

However, even if your VoIP services somehow provide you with secured connections, a VoIP solution is still vulnerable to a number of other threats. These include all of the standard network attacks, like AitM, hijacking, pharming, and denial-of-service (DoS). Plus, there are also the concerns of vishing, phreaking, fraud, and abuse.

Securing VoIP communications often involves specific application of many common security concepts:

- Use strong passwords and two-factor authentication.
- Record call logs and inspect for unusual activity.
- Block international calling.
- Outsource VoIP to a trusted SaaS.
- Update VoIP equipment firmware.
- Restrict physical access to VoIP-related networking equipment.
- Train users on VoIP security best practices.
- Prevent ghost or phantom calls on IP phones by blocking nonexistent or invalid-origin numbers.
- Implement NIPS with VoIP evaluation features.

Vishing and Phreaking

Malicious individuals can exploit voice communications through social engineering. Social engineering is a means by which an unknown, untrusted, or at least unauthorized person gains the trust of someone inside your organization in order to gain access to

information or to a system. For more on social engineering in general, see Chapter 2, “Personnel Security and Risk Management Concepts.”

VoIP services are a favorite tool of social engineers because it allows them to call anyone with little to no expense. VoIP also allows the adversary to falsify their Caller ID in order to mask their identity or establish a pretext to fool the victim. Anyone who can receive a call, whether using a traditional PSTN landline, a PBX business line, a mobile phone, or a VoIP solution, can be the target of a VoIP-originated voice-based social engineering attack. This type of attack is known as *vishing*, which stands for voice-based phishing.

The only way to protect against vishing is to teach users how to respond and interact with any form of communication. Here are some guidelines:

- Always err on the side of caution whenever voice communications seem odd, out of place, or unexpected.
- Always request proof of identity before continuing a call related to anything sensitive, personal, financial, or confidential.
- Require callback authorizations on all voice-only requests for network alterations or activities. A callback authorization occurs when the initial client connection is disconnected, and a person or party calls the client on a predetermined number that will usually be stored in a corporate directory in order to verify the identity of the client.
- Classify information (usernames, passwords, IP addresses, manager names, dial-in numbers, and so on), and clearly indicate which information can be discussed or even confirmed using voice communications.
- If privileged information is requested over the phone by an individual who should know that giving out that particular information over the phone is against the company's security policy, ask why the information is needed and verify their identity again. This incident should also be reported to the security administrator.

- Never give out or change passwords via voice-only communications.
- Block numbers that are associated with vishing.
- Don't assume that the displayed Caller ID is valid. Caller ID should be used as an indicator of who you don't want to talk to, not a confirmation of who is calling.

Malicious attackers known as *phreakers* abuse phone systems in much the same way that attackers abuse computer networks (the "ph" represents "phone"). *Phreaking* is a specific type of attack directed toward the telephone system and voice services in general. Phreakers use various types of technology to circumvent the telephone system to make free long-distance calls, alter the function of telephone service, steal specialized services, and even cause service disruptions. Some phreaker tools are actual devices, whereas others are just particular ways of using a regular telephone.

Although phreakers originally focused on PSTN phones and systems, they have evolved as voice technology has evolved. Phreakers can attack mobile devices, PBX systems, and VoIP solutions.

PBX Fraud and Abuse

Another voice communications threat is private branch exchange fraud and abuse. *Private branch exchange (PBX)* is a telephone switching or exchange system deployed in private organizations in order to enable multistation use of a small number of external PSTN lines. For example, a PBX may allow 150 phones in the office to have shared access to 20 leased PSTN lines. Many PBX systems allowed for interoffice calls without using external lines, assigned extension numbers to each handset, supported voice mail per extension, and remote calling. Remote calling, also known as hoteling, is the ability to be outside the offices, call into the office PBX system, type in a code to access a dial tone, and then dial another phone number. The original purpose of remote calling was to save money by having external personnel call the office on a toll-free number, and then make any long-distance calls on the office's long-distance calling plan.

Many PBX systems can be exploited by malicious individuals to avoid toll charges and hide their identity. Phreakers may be able to gain unauthorized access to personal voice mailboxes, redirect messages, block access, and redirect inbound and outbound calls.

Countermeasures to PBX fraud and abuse include many of the same precautions you would employ to protect a typical computer network: logical or technical controls, administrative controls, and physical controls. Here are several key points to keep in mind when designing a PBX security solution:

- Consider replacing remote access or long-distance calling through the PBX with a credit card or calling card system.
- Restrict dial-in and dial-out features to authorized individuals who require such functionality for their work tasks.
- If you still have dial-in modems, use unpublished phone numbers that are outside the prefix block range of your voice numbers.
- Protect administrative interfaces for the PBX.
- Block or disable any unassigned access codes or accounts.
- Define an acceptable use policy and train users on how to properly use the system.
- Log and audit all activities on the PBX and review the audit trails for security and use violations.
- Disable maintenance modems (i.e., remote access modems used by the vendor to remotely manage, update, and tune a deployed product) and/or any form of remote administrative access.
- Change all default configurations, especially passwords, and capabilities related to administrative or privileged features.
- Block remote dialing.
- Keep the system current with vendor/service provider updates.
- Deploy direct inward system access (DISA) technologies to reduce PBX fraud by external parties.

Direct inward system access (DISA), like any other security feature, must be properly installed, configured, and monitored in order to obtain the desired security improvement. DISA adds authentication requirements to all external connections to the PBX. Simply having DISA is not sufficient. Be sure to disable all features that are not required by the organization, craft user codes/passwords that are complex and difficult to guess, and then turn on auditing to keep watch on PBX activities.

Additionally, maintaining physical access control to all PBX connection centers, phone portals, and wiring closets prevents direct intrusion from on-site attackers. PBX systems of the past were primarily hardwar-based. Today, there are numerous PBX systems that are primarily software solutions, which may control and manage PSTN lines or VoIP connections. These software-based PBX systems are potentially vulnerable to the same application and network attacks that "standard" software and computers are subjected to, such as buffer overflows, malware, DoS, AitM attacks, hijacking, and eavesdropping. Thus, if your network is not secure, then your PBX system is likely not being securely managed either.

Remote Access Security Management

Telecommuting, or working remotely, has become a common feature of business computing. Telecommuting usually requires remote access, the ability of a distant client to establish a communication session with a network. Remote access can take the following forms (among others):

- Connecting to a network over the Internet through a VPN
- Connecting to a WAP (which the local environment treats as remote access)
- Connecting to a terminal server system, mainframe, virtual private cloud (VPC) endpoint, virtual desktop interface (VDI), or virtual mobile interface (VMI) through a thin-client connection
- Connecting to an office-located PC using a remote desktop service

- Using cloud-based virtual desktop solutions
- Using a modem to dial up directly to a remote access server

The first three examples use fully capable clients. They establish connections just as if they were directly connected to the LAN. In the last three examples, all computing activities occur on the connected central system rather than on the remote client.

Remote Access and Telecommuting Techniques

Telecommuting is performing work at a remote location (i.e., other than the primary office). In fact, there is a good chance that you perform some form of telecommuting as part of your current job. Telecommuting clients use many remote access techniques to establish connectivity to the central office LAN. There are several types of remote access techniques:

Service-Specific *Service-specific remote access* gives users the ability to connect to and manipulate or interact with a single service, such as email, remotely.

Remote Control *Remote-control remote access* grants a remote user the ability to fully control another system that is physically distant from them. The monitor and keyboard act as if they are directly connected to the remote system.

Remote Node Operation *Remote node operation* is just another name for when a remote client establishes a direct connection to a LAN, such as with wireless, VPN, or dial-up connectivity. A remote system connects to a remote access server, which provides the remote client with network services and possible Internet access.

Remote Connection Security

When remote access capabilities are deployed in any environment, security must be considered and implemented to provide protection for your private network against remote access complications:

- Remote access users should be stringently authenticated before being granted access.

- Only those users who specifically need remote access for their assigned work tasks should be granted permission to establish remote connections.
- All remote communications should be protected from interception and eavesdropping. Doing so usually requires an encryption solution that provides strong protection for the authentication traffic as well as all data transmission.

It is important to establish secure communication channels before initiating the transmission of sensitive, valuable, or personal information. Remote connections can pose several potential security concerns if not protected and monitored sufficiently:

- If anyone with a remote connection can attempt to breach the security of your organization, the benefits of physical security are reduced.
- Telecommuters might use insecure or less secure remote systems to access sensitive data and thus expose it to a greater risk of loss, compromise, or disclosure.
- Remote systems might be exposed to malicious code and could be used as a carrier to bring malware into the private LAN.
- Remote systems might be less physically secure and thus at risk of being used by unauthorized entities or stolen.
- Remote systems might be more difficult to troubleshoot, especially if the issues revolve around a remote connection.
- Remote systems might not be as easy to upgrade or patch due to their potential infrequent connections or slow throughput links. However, this issue is lessened when high-speed, reliable broadband links are present.

These issues, and likely others, need to be considered, and a remote access security policy needs to be established.

Plan a Remote Access Security Policy

When outlining your remote access security management strategy, be sure to address the following issues in the policy:

Remote Connectivity Technology Each type of connection has its own unique security issues. Fully examine every aspect of your connection options. This can include cellular/mobile services, PSTN modems, cable TV Internet services, Digital Subscriber Line (DSL), fiber connections, wireless networking, and satellite.

Transmission Protection There are several forms of encrypted protocols, encrypted connection systems, and encrypted network services or applications. Use the appropriate combination of secured services for your remote connectivity needs. This can include VPNs and/or TLS.

Authentication Protection In addition to protecting data traffic, you must ensure that all logon credentials are properly secured. This requires the use of a secure authentication protocol, may mandate the use of a centralized remote access authentication system, and should require multifactor authentication.

Remote User Assistance Remote access users may periodically require technical assistance. You must have a means established to provide this as efficiently as possible. This can include, for example, addressing software and hardware issues and user training issues. If an organization is unable to provide a reasonable solution for remote user technical support, it could result in a loss of productivity, compromise of the remote system, or an overall breach of organizational security.

If it is difficult or impossible to maintain a similar level of security on a remote system as is maintained in the private LAN, then remote access should be reconsidered in light of the security risks it represents. Network access control (NAC) can assist with this but may burden slower connections with large updates and patch transfers.

The ability to use remote access or establish a remote connection should be tightly controlled. You can control and restrict the use of remote connectivity by means of filters, rules, or access controls based on user identity, workstation identity, protocol, application, content, and time of day. (See attribute-based access control [ABAC] in Chapter 14.)

It should be a standard element in your security policy that no unauthorized modems be present on any system connected to the private network. You may need to specify this policy further by indicating that those with portable systems must either remove their modems before connecting to the network or boot with a hardware profile that disables the modem's device driver. This is the same prohibition concept that should be applied to secondary connection options of all types, including wireless and cellular.

Network Administrative Functions

Remote access does not need to focus exclusively on general workers for telecommuting. Remote access can also be an essential tool of administrators for the operation of network administrative functions. Network administrative functions encompass a range of tasks and capabilities that administrators perform to manage and control network resources from locations outside the physical infrastructure. These functions are vital for optimizing network performance, ensuring security, and responding to evolving requirements.

Configuration management is a key aspect, allowing administrators to remotely configure and modify network devices such as routers, switches, and firewalls. This involves adjusting settings, updating configurations, and implementing changes to meet the network's needs.

Monitoring and analysis are facilitated through remote access, enabling administrators to track network performance, analyze traffic patterns, and identify potential issues or security threats. Remote monitoring tools help monitor network metrics, analyze logs, and respond to alerts to ensure network health.

Troubleshooting and diagnostics benefit from remote access, as administrators can diagnose and address network issues from a remote location. This includes accessing devices, running diagnostic tests, analyzing logs, and implementing solutions to resolve connectivity or performance problems.

Security management involves configuring security policies, access controls, and authentication mechanisms remotely to protect the

network. Administrators can manage firewalls, VPNs, and other security measures to safeguard the network infrastructure.

User account management is streamlined with remote access, allowing administrators to create, modify, or deactivate user accounts, reset passwords, and control access rights to network resources.

Software updates and patch management can be performed remotely, with administrators deploying updates, patches, and security fixes to network devices and servers. This helps address vulnerabilities and ensures that the network operates with the latest features and security enhancements.

Backup and recovery tasks are facilitated through remote access, enabling administrators to schedule remote backups, verify data integrity, and implement recovery procedures in case of data loss or system failures.

Policy enforcement involves administrators ensuring that network configurations align with organizational policies, security standards, and industry regulations. This is done remotely to enforce compliance and maintain a secure network environment.

Remote access network administrative functions are essential for maintaining operational efficiency, responding to issues promptly, and ensuring the overall health and security of network infrastructure, especially in scenarios where physical presence at the network site is not feasible. Any and all remote access-based administrative functions and their necessary security requirements should be defined in an organizational security policy.

Multimedia Collaboration

Multimedia collaboration is the use of various multimedia-supporting communication solutions to enhance distance collaboration (people working on a project together remotely). Often, collaboration allows workers to work simultaneously as well as across different time frames. Collaboration can also be used to track changes and include multimedia functions. Collaboration can incorporate email, chat, voice/VoIP, video/video conferencing, use of

a whiteboard, online document editing, real-time file exchange, versioning control, and other tools. It is often a feature of advanced forms of remote meeting technology.

Whatever SaaS service is implemented to support multimedia collaboration, it is essential that it be thoroughly reviewed against the organization's security policy. Just because someone is working remotely does not mean that security should be relaxed. It is important to verify that connections are encrypted, that robust multifactor authentication is in use, and that tracking is available for the hosting organization to review.

One means to support remote access and collaboration activities is through the use of online conferencing solutions. One such product is Zoom, which gained extreme popularity in 2020 due to the pandemic lockdowns that resulted in many employees needing to continue working from home. Zoom is only one of several video conferencing products available.

Now that many employees have returned to the office, there is still a significant need for online remote video conferencing and collaboration. Some organizations have established Zoom rooms. A *Zoom room* refers to a dedicated physical space equipped with audio-visual and communication technology designed for hosting video meetings, conferences, and collaborations. A Zoom room is set up to enhance the quality and experience of online video collaboration meetings. They often include larger displays, high-quality camera and microphone equipment, a quality sound system, touchscreen system/room controls, lighting controls, and other smart technologies.

The concept of a Zoom room is part of the broader trend toward creating collaborative and technology-enabled meeting spaces within workplaces. It allows for a more immersive and effective collaboration experience during virtual meetings, particularly in settings where teams or groups gather for discussions, presentations, or remote interactions.

Remote Meeting

Remote meeting technology is used for any product, hardware, or software that allows for interaction between remote parties. These technologies and solutions are known by many other terms: digital collaboration, virtual meetings, videoconferencing, software or application collaboration, shared whiteboard services, virtual training solutions, and so on. Any service that enables people to communicate, exchange data, collaborate on materials/data/documents, and otherwise perform work tasks together can be considered a remote meeting technology service.

No matter what form of multimedia collaboration is implemented, the attendant security implications must be evaluated. There are many questions about security that need to be asked and satisfactory answers uncovered prior to deployment or use:

- Does the service use strong authentication techniques?
- Does the communication occur across an open protocol or an encrypted tunnel?
- Is the encryption just from the endpoint to the central server, or is it end-to-end?
- Does the solution allow for true deletion of content?
- Are the activities of users audited and logged?
- Can unauthorized entities join in a private meeting?
- Can attendees interject into the meeting with voice, image, video, or file sharing?
- Does the platform integrate advertising/spam into the interface, and can it be disabled?
- What tracking mechanisms are used, can the tracking be disabled, and what is the data collected for?
- Are sessions recorded? Who has access to the recordings? Can they be exported and distributed?

Multimedia collaboration and other forms of remote meeting technology can improve the work environment and allow for input

from a wider range of diverse workers across the globe, but this is a benefit only if the security of the communications solution can be ensured and personnel are trained to use it effectively and in compliance with company policy.

Instant Messaging and Chat

Instant messaging (IM), real-time messaging, or chat is a mechanism that allows for real-time text-based chat between two or more people located anywhere on the Internet. Some IM utilities allow for file transfer, multimedia, voice and videoconferencing, and more. Some forms of IM are based on a peer-to-peer service, whereas others use a centralized controlling server. Peer-to-peer-based IM and cloud-based IM systems are easy for end users to deploy and use, but it's difficult to manage from a corporate perspective because it may lack security or management controls. Messaging systems and chat services usually have numerous vulnerabilities, such as being susceptible to packet sniffing/eavesdropping, lacking native security capabilities such as multifactor authentication and encryption, and providing little or no protection for privacy.

Many stand-alone chat clients have been susceptible to malicious code deposits or infection through their file transfer capabilities. Also, chat users are often subject to numerous forms of social engineering attacks, such as impersonation or convincing a victim to reveal information that should remain confidential (such as passwords, PII, or intellectual property).

When selecting collaboration products, always consider the locus of control and the availability and effectiveness of security features, such as logging, multifactor authentication, and transmission encryption.

Monitoring and Management

Monitoring and management in the context of network operations involve various practices and tools aimed at ensuring the reliability, performance, and security of a network. Network observability, a key aspect, refers to the ability to gain insights into the internal state of a network by collecting and analyzing relevant data. This involves

monitoring various metrics, logs, and traces to understand how the network components are performing. The purpose is to enhance visibility into network behavior, detect issues, and gain actionable insights to optimize performance and troubleshoot problems.

Another critical area is traffic flow/shaping, which involves managing the flow of data within a network to optimize performance, allocate resources efficiently, and ensure a consistent user experience. By shaping traffic, administrators can prioritize certain types of data, manage bandwidth usage, and control the flow of information to prevent congestion or bottlenecks.

Capacity management is the practice of planning, monitoring, and optimizing the network's capacity to ensure it can handle current and future demands effectively. By monitoring resource usage and predicting future needs, administrators can allocate resources appropriately, prevent performance degradation, and ensure scalability.

Fault detection and handling involve identifying and addressing issues, errors, or failures within the network. The goal is to detect problems as soon as possible, minimize downtime, and implement strategies for fault tolerance and resilience. Automated alerts and notifications can aid in a prompt response to faults.

Monitoring and management in networking encompass practices related to network observability, traffic flow/shaping, capacity management, and fault detection and handling. These practices collectively contribute to maintaining a healthy and efficient network infrastructure, ensuring that it meets performance expectations, is resilient to faults, and can adapt to changing demands. Advanced tools and technologies, such as network monitoring software, traffic shaping mechanisms, and predictive analytics, play a crucial role in implementing effective monitoring and management strategies in modern network environments.

Load Balancing

The purpose of *load balancing* is to obtain more optimal infrastructure utilization, minimize response time, maximize throughput, reduce overloading, and eliminate bottlenecks. A *load*

balancer is used to spread or distribute network traffic load across several network links or network devices. Although load balancing can be used in a variety of situations, a common implementation is spreading a load across multiple members of a server farm or cluster. Scheduling or load-balancing methods are the means by which a load balancer distributes the work, requests, or loads among the devices behind it. A load balancer might use a variety of scheduling techniques to perform load distribution, as described in Table 12.1.

TABLE 12.1 Common load-balancing scheduling techniques

Technique	Description
Random choice	Each packet or connection is assigned a destination randomly.
Round robin	Each packet or connection is assigned the next destination in order, such as 1, 2, 3, 4, 5, 1, 2, 3, 4, 5, and so on.
Load monitoring	Each packet or connection is assigned a destination based on the current load or capacity of the targets. The device/path with the lowest current load receives the next packet or connection.
Preferencing or weighted	Each packet or connection is assigned a destination based on a subjective preference or known capacity difference. For example, suppose system 1 can handle twice the capacity of systems 2 and 3; in this case, preferencing would look like 1, 2, 1, 3, 1, 2, 1, 3, 1, and so on.
Least connections/traffic/latency	Each packet or connection is assigned a destination based on the least number of active connections, traffic load, or latency.
Locality based (geographic)	Each packet or connection is assigned a destination based on the destination's relative distance from the load balancer (used when cluster members are geographically separated or across numerous router hops).
Locality based (affinity)	Each packet or connection is assigned a destination based on previous connections from the same client, so subsequent requests go to the same

Technique	Description
	destination to optimize continuity of service. Aka persistence.

Load balancing can be either a software service or a hardware appliance. Load balancing can also incorporate many other features, depending on the protocol or application, including caching, TLS offloading, compression, buffering, error checking, filtering, and even firewall and IDS capabilities.

TLS offloading is the process of removing the TLS-based encryption from incoming traffic to relieve a web server of the processing burden of decrypting and/or encrypting traffic sent.

Virtual IP Addresses

In load-balancing scenarios, virtual IP addresses (VIP or VIPA) serve as key components to efficiently distribute incoming network traffic across multiple servers or resources. Unlike a physical IP address associated with a specific network interface, a VIP is mapped to a cluster or group of servers. When clients access the VIP, a load balancer directs their requests to one of the servers in the pool, ensuring that the overall load is evenly distributed and preventing any single server from becoming a bottleneck.

Load balancers utilize virtual IP addresses as the entry point for incoming traffic, making decisions on how to distribute the load based on defined algorithms or balancing schedules. The result is an optimized distribution of client requests across the backend servers, contributing to efficient resource utilization.

One significant advantage of virtual IP addresses in load balancing is their role in enhancing high availability. In the event of a server failure, the load balancer can seamlessly redirect traffic to other healthy servers, minimizing downtime and ensuring continuous service availability. This redundancy and failover capability are

crucial for maintaining uninterrupted service in dynamic and scalable environments.

Virtual IP addresses also facilitate scalability by allowing the dynamic addition or removal of servers in response to changes in infrastructure size. As the system scales, load balancers adapt to the evolving server pool, and clients can access the service through the virtual IP address without being affected by modifications in the backend server configuration.

Load balancers often handle SSL/TLS termination at the virtual IP address, decrypting incoming encrypted traffic before distributing it to backend servers. Additionally, virtual IP addresses can be associated with content switching, enabling the load balancer to route traffic based on content types or specific application services.

In Global Server Load Balancing (GSLB) scenarios, virtual IP addresses play a crucial role in distributing traffic across multiple data centers or locations on a global scale. This approach considers factors such as proximity, server health, or other criteria to optimize both performance and reliability on a global level.

Virtual IP addresses are fundamental in load balancing architectures, providing a versatile and efficient mechanism for directing incoming traffic to backend servers. Their role spans from optimizing resource utilization and enhancing high availability to supporting scalability and global server load balancing.

Active-Active vs. Active-Passive

An *active-active system* is a form of load balancing that uses all available pathways or systems during normal operations. In the event of a failure of one or more of the pathways, the remaining active pathways must support the full load that was previously handled by all. This technique is used when the traffic levels or workload during normal operations need to be maximized (i.e., optimizing availability), but reduced capacity will be tolerated during adverse conditions (i.e., reducing availability).

An *active-passive system* is a form of load balancing that keeps some pathways or systems in an unused dormant state during normal operations. If one of the active elements fails, then a passive element

is brought online and takes over the workload for the failed element. This technique is used when the level of throughput or workload needs to be consistent between normal states and adverse conditions (i.e., maintaining availability consistency).

Manage Email Security

Email is one of the most widely and commonly used Internet services. The email infrastructure employed on the Internet primarily consists of email servers using *Simple Mail Transfer Protocol (SMTP)* (TCP port 25) to accept messages from clients, transport those messages to other servers, and deposit them into a user's server-based inbox. In addition to email servers, the email infrastructure includes email clients. Clients retrieve email from their server-based inboxes using *Post Office Protocol version 3 (POP3)* (TCP port 110) or *Internet Message Access Protocol (IMAP)* (technically version 4) (TCP port 143). Internet-compatible email systems rely on the X.400 standard for addressing and message handling.

Postfix is the most common SMTP server for Unix systems (replacing the previously popular Sendmail product), and Exchange is the most common SMTP server for Microsoft systems. In addition to these popular products, numerous alternatives exist, but they all share the same basic functionality and compliance with Internet email standards.

If you deploy an SMTP server, it is imperative that you properly configure strong authentication for both inbound and outbound mail. SMTP is designed to be a mail relay system. This means it relays mail from the sender to the intended recipient. However, you want to avoid turning your SMTP server into an *open relay* (also known as an open relay agent or *relay agent*), which is an SMTP server that does not authenticate senders before accepting and relaying mail. Open relays are prime targets for spammers because they allow spammers to send out floods of emails by piggybacking on an insecure email infrastructure. As open relays are locked down—becoming *closed relays* or *authenticated relays*—adversaries are

often resorting to hijacking authenticated user accounts through social engineering or credential stuffing/spraying/guessing attacks.

Another option to consider for corporate email is an SaaS email solution. Examples of cloud or hosted email include Gmail (Google Workspace) and Outlook/Exchange Online. SaaS email enables you to leverage the security experience and management expertise of some of the largest email service providers to support your company's communications. Benefits of SaaS email include high availability, distributed architecture, ease of access, standardized configuration, and physical location independence. However, there are some potential risks with using a hosted email solution, including block listing issues, rate limiting, app/add-on restrictions, and what (if any) additional security mechanisms you can deploy.

Email Security Goals

The basic email mechanisms in use on the Internet offer efficient delivery of messages but lack controls to provide for confidentiality, integrity, or even availability. In other words, basic email is not secure. However, you can add security to email in many ways. Adding security to email may satisfy one or more of the following objectives:

- Restrict access to messages to their intended recipients (i.e., privacy and confidentiality).
- Maintain the integrity of messages.
- Authenticate and verify the source of messages.
- Provide for nonrepudiation.
- Verify the delivery of messages.
- Classify sensitive content within or attached to messages.

There is no real method to guarantee the availability of email, such as access to an inbox or assured delivery. However, these can be compensated for using verified delivery and maintaining several access vectors from clients to email servers (such as LAN, general Internet, and mobile data services).

As with any aspect of IT security, email security begins in a security policy approved by upper management. Within the security policy, you must address several issues:

- Acceptable use policies for email
- Access control and privacy
- Email management
- Email backup and retention policies

Acceptable use policies define what activities can and cannot be performed over an organization's email infrastructure. It is often stipulated that professional, business-oriented emails and a limited amount of personal emails can be sent and received through company-owned or provided email systems. Specific restrictions are usually placed on performing personal business (i.e., work for another organization, including self-employment) and sending or receiving illegal, immoral, or offensive communications as well as engaging in any other activities that would have a detrimental effect on productivity, profitability, or public relations.

Access control over email should be maintained so that users have access only to their specific inbox and email archive databases. An extension of this rule implies that no other user, authorized or not, can gain access to an individual's email. Access control should provide for both legitimate access and some level of privacy, at least from other employees and unauthorized intruders.

The mechanisms and processes used to implement, maintain, and administer email for an organization should be clarified. End users may not need to know the specifics of email management, but they do need to know whether email is considered private communication.

Email has recently been the focus of numerous court cases in which archived messages were used as evidence—often to the chagrin of the author or recipient of those messages. If email is to be retained (that is, backed up and stored in archives for future use), users need to be made aware of this. If email is to be reviewed for violations by an auditor, users need to be informed of this as well. Some companies

have elected to retain only the last three months of email archives before they are destroyed, whereas others have opted to retain email for years. Depending on your country and industry, there are often regulations that dictate retention policies. But keep in mind, that although your organization may discard sent or received messages after only a few months, external entities may retain their copies of the conversations for years. The details of an email retention policy may need to be shared with affected subjects, which may include privacy implications, how long the messages are maintained, and for what purposes the messages can be used (such as auditing or violation investigations).

Understand Email Security Issues

The first step in deploying email security is to recognize the vulnerabilities specific to email. The standard protocols used to support email (i.e., SMTP, POP3, and IMAP) do not employ encryption natively. Thus, all messages are transmitted in the form in which they are submitted to the email server, which is often plaintext. This makes interception and eavesdropping easy.

Email is a common delivery mechanism for viruses, worms, Trojan horses, documents with destructive macros, and other malicious code. The proliferation of support for various scripting languages, auto-download capabilities, and auto-execute features has transformed hyperlinks within the content of email and attachments into a serious threat to every system. Many email clients now natively support HTML code (and thus JavaScript), which may be rendered automatically when a message is accessed.

Email offers little in the way of native source verification. Spoofing the source address of an email is a simple process for even a novice attacker. Email headers can be modified at their source or at any point during transit. Furthermore, it is also possible to deliver email directly to a user's inbox on an email server by directly connecting to the email server's SMTP port. And speaking of in-transit modification, there are no native integrity checks to ensure that a message was not altered between its source and destination.

In addition, email itself can be used as an attack mechanism. When sufficient numbers of messages are directed to a single user's inbox

or through a specific SMTP server, a DoS attack can result. This attack is often called mail-bombing and is simply a DoS performed by inundating a system with messages. The DoS can be the result of storage capacity consumption or processing capability utilization. Either way, the result is the same: legitimate messages cannot be delivered.

A similar DoS issue is called a *mail storm*. This is when someone responds with a Reply All to a message that has a significant number of other recipients in the To: and CC: lines. As others receive these replies, they, in turn, use Reply All with their comments or demands to be removed from the conversation. This is further exacerbated if recipients have auto-responders set to Reply All for out-of-office notifications or other announcements.

Like email flooding and malicious code attachments, unwanted email can be considered an attack. Sending unwanted, inappropriate, or irrelevant messages is called spamming. Spamming is often little more than a nuisance, but it does waste system resources both locally and over the Internet. It is often difficult to stop spam because the source of the messages is usually spoofed.

Email Security Solutions

Imposing security on email is possible, but the efforts should be in tune with the value and confidentiality of the messages being exchanged. You can use several protocols, services, and solutions to add security to email without requiring a complete overhaul of the entire Internet-based SMTP infrastructure. Many of these email security improvements are forms of encryption; see Chapter 6, "Cryptography and Symmetric Key Algorithms," and Chapter 7, "PKI and Cryptographic Applications," for information on cryptography.

Secure Multipurpose Internet Mail Extensions (S/MIME)
S/MIME is an email security standard that offers authentication and confidentiality to email through public key encryption, digital envelopes, and digital signatures. Authentication is provided through X.509 digital certificates issued by trusted third-party CAs. Privacy is provided through the use of Public Key Cryptography Standard (PKCS) standards-compliant encryption. Two types of messages can be formed using S/MIME: signed messages and secured enveloped

messages. A signed message provides integrity, sender authentication, and nonrepudiation. An enveloped message provides recipient authentication and confidentiality.

Pretty Good Privacy (PGP) PGP is a peer-to-peer public-private key–based email system that uses a variety of encryption algorithms to encrypt files and email messages. PGP is not a standard but rather an independently developed product that has wide Internet grassroots support, which has elevated its proprietary certificates to de facto standard status.

DomainKeys Identified Mail (DKIM) DKIM is an email authentication method designed to verify the authenticity of the sender of an email message. It allows the recipient's mail server to check that an email claiming to come from a specific domain was indeed authorized by the owner of that domain. DKIM helps combat email spoofing, phishing, and other forms of email fraud by providing a way to verify the integrity of the email's origin. See `http://dkim.org`.

Sender Policy Framework (SPF) To protect against spam and email spoofing, an organization can also configure its SMTP servers for Sender Policy Framework (SPF). SPF operates by checking that inbound messages originate from a host authorized to send messages by the owners of the SMTP origin domain. For example, if you receive a message from `mark.nugget@abccorps.com`, then SPF checks with the administrators of `smtp.abccorps.com` that `mark.nugget` is authorized to send messages through their system before the inbound message is accepted and sent into your recipient's inbox.

Domain-based Message Authentication Reporting and Conformance (DMARC) DMARC is a DNS-based email authentication system. It is an email authentication and policy framework that builds on the SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) protocols. DMARC allows domain owners to specify how their emails should be authenticated, how failed authentication should be handled, and how feedback about email activity should be provided. DMARC is intended to protect against business email compromise (BEC), phishing, and other email scams. Email servers can verify if a received message is

valid by following the DNS-based instructions; if invalid, the email can be discarded, quarantined, or delivered anyway.

STARTTLS A lot of organizations are using Secure SMTP over TLS nowadays; however, it's not as widespread as it should be. STARTTLS (aka *explicit TLS* or *opportunistic TLS* for SMTP) will attempt to set up an encrypted connection with the target email server in the event that it is supported. STARTTLS is not a protocol but instead an SMTP command. Once the initial SMTP connection is made to the email server, the STARTTLS command will be used. If the target system supports TLS, then an encrypted channel will be negotiated. Otherwise, it will remain as plaintext. STARTTLS's secure session will take place on TCP port 587. STARTTLS can also be used with IMAP connections, whereas POP3 connections use the STLS command to perform a similar function.

Implicit SMTPS This is the TLS-encrypted form of SMTP, which assumes the target server supports TLS. If accurate, then an encrypted session is negotiated. If not, then the connection is terminated because plaintext is not accepted. SMTPS communications are initiated against TCP port 465.

Free PGP Solution

PGP started off as a free product for all to use, but it has since splintered into various divergent products. PGP is a commercial product, whereas OpenPGP is a developing standard that GnuPG is compliant with and that was independently developed by the Free Software Foundation. If you have not used PGP before, we recommend downloading the appropriate GnuPG version for your preferred email platform. This secure solution is sure to improve your email privacy and integrity. You can learn more about GnuPG at http://gnupg.org. You can learn more about PGP by visiting its pages on Wikipedia.

By using these and other security mechanisms for email and communication transmissions, you can reduce or eliminate many of the security vulnerabilities of email. Digital signatures can help eliminate impersonation. The encryption of messages reduces

eavesdropping. And the use of email filters keeps spamming and mail-bombing to a minimum.

Blocking attachments at the email gateway system on your network can ease the threats from malicious attachments. You can have a 100 percent no-attachments policy or block only attachments that are known or suspected to be malicious, such as attachments with extensions that are used for executable and scripting files. If attachments are an essential part of your email communications, you'll need to train your users and use antimalware tools for protection. Training users to avoid contact with suspicious or unexpected attachments greatly reduces the risk of malicious code transference via email. Antimalware products are generally effective against known malicious code, but they offer little protection against new or unknown varieties.

Unwanted emails can be a hassle, a security risk, and a drain on resources. Whether spam, malicious email, or just bulk advertising, there are several ways to reduce the impact on your infrastructure. Block list services offer a subscription system to a list of known email abuse sources. You can integrate the block list into your email server so that any messages originating from a known abusive domain or IP address are automatically discarded. Another option is to use a challenge/response filter. In these services, when an email is received from a new/unknown origin address, an autoresponder sends a request for a confirmation message. Spammers and auto-emailers will not respond to these requests, but valid humans will. Once they have confirmed that they are human and agree not to spam the destination address, their source address is added to an allow list for future communications.

Unwanted email can also be managed through the use of email *reputation filtering*. Several services maintain a grading system of email services in order to determine which are used for standard/normal communications and which are used for spam. These services include Sender Score, Cisco SenderBase Reputation Service, Broadcom's Symantec Email Security.cloud, Spamhaus ZEN, and Barracuda Reputation Block List (BRBL). These and other mechanisms are used as part of several spam filtering technologies, such as Apache SpamAssassin and spamd.

Fax Security

Fax communications are waning in popularity because of the widespread use of email. Even with declining use, faxes still represent a communications path that is vulnerable to attack. Like any other telephone communication, faxes can be intercepted and are susceptible to eavesdropping.

Some of the mechanisms that can be deployed to improve the security of faxes are fax encrypters, link encryption, activity logs, and exception reports. A fax encrypter gives a fax machine the capability to use an encryption protocol to scramble the outgoing fax signal. Link encryption is the use of an encrypted communication path, like a VPN link or a secured telephone link, to transmit the fax. Activity logs and exception reports can be used to detect anomalies in fax activity that could be symptoms of an attack.

In addition to the security of a fax transmission, it is important to consider the security of a received fax. Faxes that are automatically printed may sit in the out tray for a long period of time, therefore making them subject to viewing by unintended recipients. Studies have shown that adding banners of CONFIDENTIAL, PRIVATE, and so on spur the curiosity of passersby. So, disable automatic printing. Also, avoid fax machines that retain a copy of the fax in memory or on a local storage device. Consider integrating your fax system with your network so that you can email faxes to intended recipients instead of printing them to paper.

Virtual Private Network

A *virtual private network (VPN)* is a communication channel between two entities across an intermediary untrusted network. VPNs can provide several critical security functions, such as access control, authentication, confidentiality, and integrity. Most VPNs use encryption to protect the encapsulated traffic, but encryption is not

necessary for the connection to be considered a VPN. A VPN is an example of a virtualized network.

VPNs are most commonly associated with establishing secure communication paths through the Internet between two distant networks. However, they can exist anywhere, including within private networks or between end-user systems connected to an ISP. The VPN can link two networks or two individual systems. They can link clients, servers, routers, firewalls, and switches. VPNs are also helpful in providing security for legacy applications that rely on risky or vulnerable communication protocols or methodologies, especially when communication is across a network.

Although VPNs can provide confidentiality and integrity over insecure or untrusted intermediary networks, they do not provide or guarantee availability. VPNs are also in relatively widespread use to get around location requirements for services like Netflix and Hulu and thus provide a (at times questionable) level of anonymity.

A *VPN concentrator* is a dedicated hardware device designed to support a large number of simultaneous VPN connections, often hundreds or thousands. It provides high availability, high scalability, and high performance for secure VPN connections. A VPN concentrator can also be called a *VPN server*, a *VPN gateway*, a *VPN firewall*, a *VPN remote access server (RAS)*, a *VPN device*, a *VPN proxy*, or a *VPN appliance*. The use of VPN devices is transparent to networked systems. Therefore, individual hosts do not need to support VPN capabilities locally if a VPN appliance is present.

Tunneling

Before you can truly understand VPNs, you must first grasp the concept of tunneling. *Tunneling* is the network communications process that protects the contents of protocol packets by encapsulating them in packets of another protocol. The encapsulation is what creates the logical illusion of a communications tunnel over the untrusted intermediary network. This virtual path exists between the encapsulation and the deencapsulation entities located at the ends of the communication.

As data is transmitted from one system to another across a VPN link, the normal LAN TCP/IP traffic is encapsulated (encased or enclosed) in the VPN protocol. The VPN protocol acts like a security envelope that provides special delivery capabilities (for example, across the Internet) as well as security mechanisms (such as data encryption).

In fact, sending a snail mail letter to your grandmother involves the use of a tunneling system. You create the personal letter (the primary content protocol packet) and place it in an envelope (the tunneling protocol). The envelope is delivered through the postal service (the untrusted intermediary network) to its intended recipient. You can use tunneling in many situations, such as when you're bypassing firewalls, gateways, proxies, or other traffic control devices. The bypass is achieved by encapsulating the restricted content inside packets that are authorized for transmission. The tunneling process prevents the traffic control devices from blocking or dropping the communication because such devices don't know what the packets actually contain.

Tunneling is often used to enable communications between otherwise disconnected systems. If two systems are separated by a lack of network connectivity, a communication link can be established by a modem dial-up link or other remote access or wide area network (WAN) networking service. The actual LAN traffic is encapsulated in whatever communication protocol is used by the temporary connection, such as Point-to-Point Protocol in the case of modem dial-up. If two networks are connected by a network employing a different protocol, the protocol of the separated networks can often be encapsulated within the intermediary network's protocol to provide a communication pathway.

Regardless of the actual situation, tunneling protects the contents of the inner protocol and traffic packets by encasing, or wrapping, it in an authorized protocol used by the intermediary network or connection. Tunneling can be used if the primary protocol is not routable and to keep the total number of protocols supported on the network to a minimum.

If the act of encapsulating a protocol involves encryption, tunneling can provide a means to transport sensitive data across untrusted

intermediary networks without fear of losing confidentiality and integrity.

Tunneling is not without its problems. It is generally an inefficient means of communicating because most protocols include their own error detection, error handling, acknowledgment, and session management features, so using more than one protocol at a time compounds the overhead required to communicate a single message. Furthermore, tunneling creates either larger packets or additional packets that in turn consume additional network bandwidth. Tunneling can quickly saturate a network if sufficient bandwidth is not available. In addition, tunneling is a point-to-point communication mechanism and is not designed to handle broadcast traffic.

Tunneling also makes it difficult, if not impossible, to monitor the contents of the traffic in some circumstances, creating issues for security practitioners. When firewalls, intrusion detection systems, malware scanners, or other packet-filtering and packet-monitoring security mechanisms are used, you must realize that the data payload of VPN traffic won't be viewable, accessible, scannable, or filterable, because it's encrypted. Thus, for these security mechanisms to function against VPN-transported data, they must be placed outside of the VPN tunnel to act on the data after it has been decrypted and returned to normal LAN traffic.

How VPNs Work

A VPN link can be established over any other network communication connection. Examples include a typical LAN cable connection, a wireless LAN connection, a remote access dial-up connection, a WAN link, or even a client using an Internet connection for access to an office LAN. A VPN link acts just like a typical direct LAN cable connection; the only possible difference would be speed based on the intermediary network and on the connection types between the client system and the server system. Over a VPN link, a client can perform the same activities and access the same resources as if they were directly connected via a LAN cable. This remote access method is known as remote node operation.

VPNs can connect two individual systems or two entire networks. The only difference is that the transmitted data is protected only while it is within the VPN tunnel. Remote access servers or firewalls on the network's border act as the start points and endpoints for VPNs. Thus, traffic is unprotected within the source LAN, protected between the border VPN servers, and then unprotected again once it reaches the destination LAN.

VPN links through the Internet for connecting to distant networks are often inexpensive alternatives to direct links or leased lines. The cost of two high-speed Internet links to local ISPs to support a VPN is often significantly less than the cost of any other connection means available.

VPNs can operate in two modes: *transport mode* and *tunnel mode*.

Transport mode links or VPNs are anchored or end at the individual hosts connected together. Let's use IPSec as an example (more on IPSec later in this chapter). In transport mode, IPSec provides encryption protection for just the payload and leaves the original message header intact (see Figure 12.1). This type of VPN is also known as a *host-to-host VPN* or an *end-to-end encrypted VPN*, since the communication remains encrypted while it is in transit between the connected hosts. Since transport mode VPNs do not encrypt a communication's header, this mode is best used only within a trusted network between individual systems. When needing to cross untrusted networks or link to and/or from multiple systems, then tunnel mode should be used.

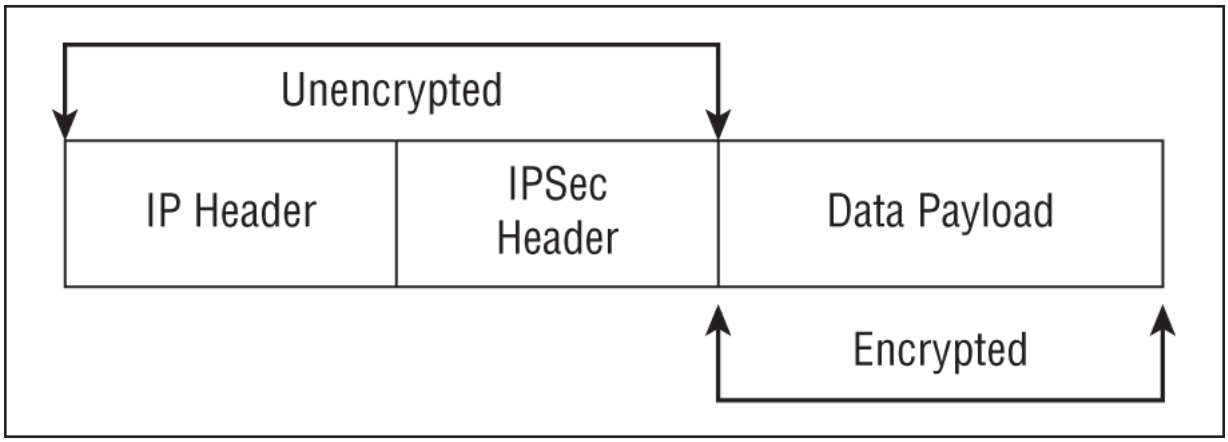

FIGURE 12.1 IPSec's encryption of a packet in transport mode

Tunnel mode links or VPNs terminate (i.e., are anchored or end) at VPN devices on the boundaries of the connected networks (or one remote device). In tunnel mode, IPSec provides encryption protection for both the payload and message header by encapsulating the entire original LAN protocol packet and adding its own temporary IPSec header (see Figure 12.2).

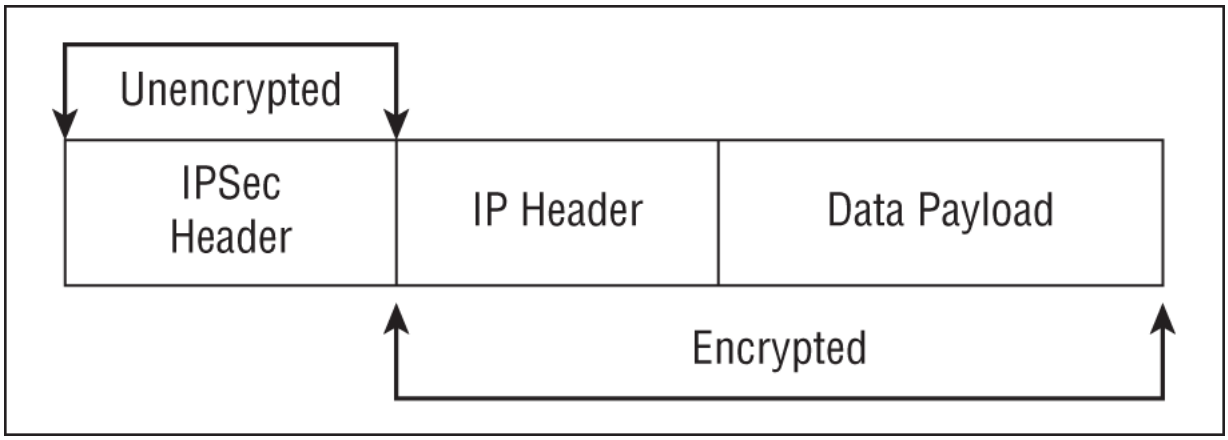

FIGURE 12.2 IPSec's encryption of a packet in tunnel mode

Numerous scenarios lend themselves to the deployment of tunnel mode VPNs; for example, VPNs can be used to connect two networks across the Internet (see Figure 12.3) (aka site-to-site VPN) or to allow distant clients to connect to an office local area network (LAN) across the Internet (see Figure 12.4) (aka remote access VPN). Once a VPN link is established, the network connectivity for the VPN client is the same as a local LAN connection. A *remote access VPN* is a variant of the *site-to-site VPN*. This type of VPN is also known as a

link encryption VPN, since encryption is only provided when the communication is in the VPN link or portion of the communication. There may be network segments before and after the VPN, which are not secured by the VPN.

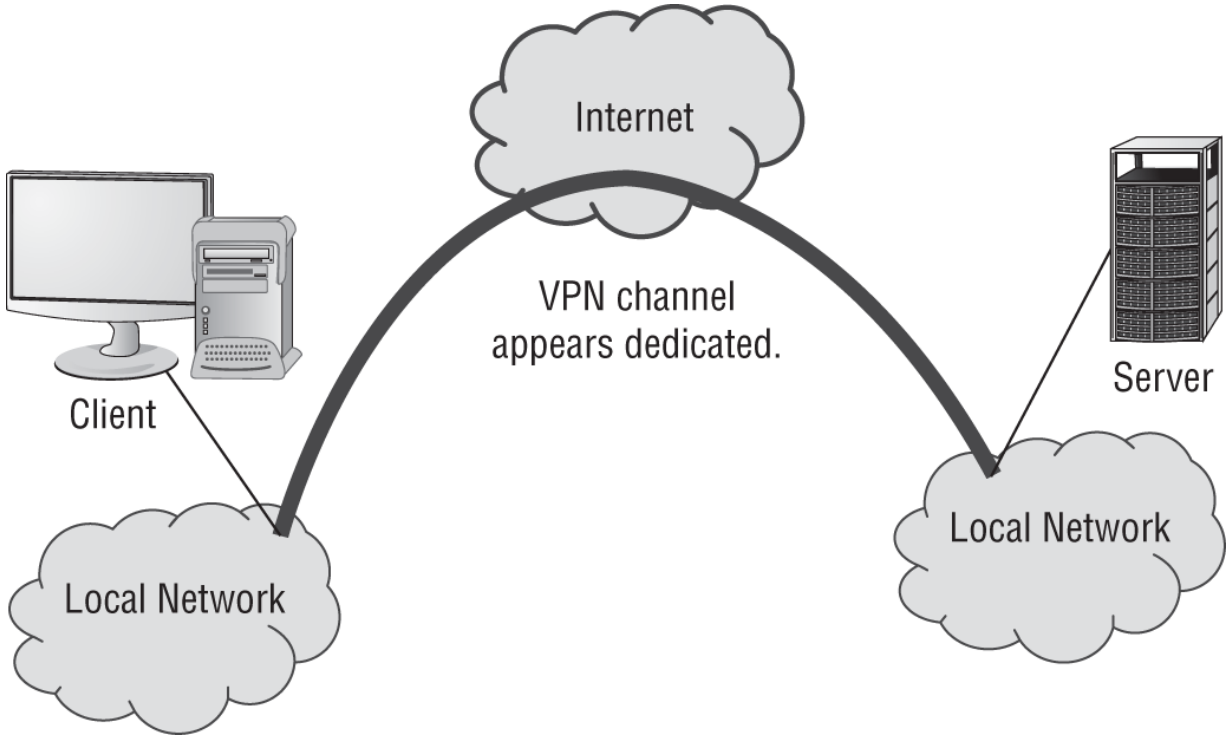

FIGURE 12.3 Two LANs being connected using a tunnel-mode VPN across the Internet

A *wide area network (WAN)* is a network over a long distance. A *metropolitan area network (MAN)* is a network within a town or city. A *campus area network (CAN)* is a network within a college campus or a business park. A VPN can be used over any type of network.

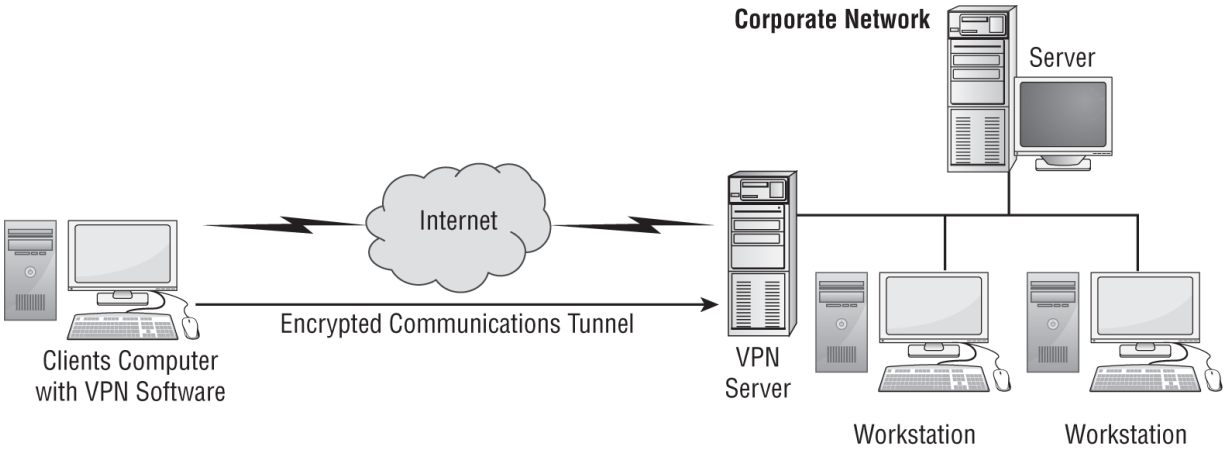

FIGURE 12.4 A client connecting to a network via a remote-access/tunnel VPN across the Internet

Always-On

An *always-on VPN* is one that attempts to auto-connect to the VPN service every time a network link becomes active. Always-on VPNs are mostly associated with mobile devices. Some always-on VPNs can be configured to engage only when an Internet link is established rather than a local network link or only when a Wi-Fi link is established rather than a wired link. Due to the risks of using an open public Internet link, whether wireless or wired, having an always-on VPN will ensure that a secure connection is established every time when attempting to use online resources.

Split Tunnel vs. Full Tunnel

A *split tunnel* is a VPN configuration that allows a VPN-connected client system (i.e., remote node) to access both the organizational network over the VPN and the Internet directly at the same time. The split tunnel thus simultaneously grants an open connection to the Internet and to the organizational network. This is usually considered a security risk for the organizational network since, when a split-tunnel VPN is established, an open pathway exists from the Internet through the client to the LAN. With a VPN connection to the LAN, the client is considered trusted, so filtering is not often used. Clients don't usually have the best filtering services themselves. So, this split tunnel pathway is an easier means for transference of

malicious code, initiating intrusions, or exfiltrating confidential data than the direct LAN-to-Internet link, which is filtered by a firewall.

A *full tunnel* is a VPN configuration in which all of the client's traffic is sent to the organizational network over the VPN link, and then any Internet-destined traffic is routed out of the organizational network's proxy or firewall interface to the Internet. A full tunnel ensures that all traffic is filtered and managed by the organizational network's security infrastructure.

Common VPN Protocols

VPNs can be implemented using software or hardware solutions. In either case, there are several common VPN protocols: PPTP, L2TP, SSH, OpenVPN (i.e., TLS), and IPSec.

Point-to-Point Tunneling Protocol

Point-to-Point Tunneling Protocol (PPTP) is an obsolete encapsulation protocol developed from the dial-up Point-to-Point Protocol. It operates at the Data Link Layer (Layer 2) of the OSI model and is used on IP networks. PPTP uses TCP port 1723. PPTP offers protection for authentication traffic through the same authentication protocols supported by PPP:

- Password Authentication Protocol (PAP)
- Challenge Handshake Authentication Protocol (CHAP)
- Extensible Authentication Protocol (EAP)
- Microsoft Challenge Handshake Authentication Protocol (MS-CHAPv2)

The initial tunnel negotiation process used by PPTP is not encrypted. Thus, the session establishment packets that include the IP address of the sender and receiver—and can include usernames and hashed passwords—could be intercepted by a third party. Most modern uses of PPTP have adopted the Microsoft customized implementation (MS-CHAPv2), which supports session encryption using Microsoft Point-to-Point Encryption (MPPE) and supports various secure

authentication options. Although PPTP is obsolete, many OSs and VPN services still support it.

Layer 2 Tunneling Protocol (L2TP)

Layer 2 Tunneling Protocol (L2TP) was developed by combining features of PPTP and Cisco's Layer 2 Forwarding (L2F) VPN protocol. Since its development, L2TP has become an Internet standard (RFC 2661). Obviously, L2TP operates at Layer 2 and thus can support just about any Layer 3 networking protocol. L2TP uses UDP port 1701.

L2TP can rely on PPP's supported authentication protocols, specifically IEEE 802.1X, which is a derivative of EAP from PPP. IEEE 802.1X enables L2TP to leverage or borrow authentication services from any available AAA server on the network, such as RADIUS or TACACS+. L2TP does not offer native encryption, but it supports the use of payload encryption protocols. Although it isn't required, L2TP is most often deployed using IPSec's ESP for payload encryption.

Generic Routing Encapsulation (GRE) is also a proprietary Cisco tunneling protocol that can be used to establish VPNs. GRE provides encapsulation but not encryption.

SSH

Secure Shell (SSH) is a secure replacement for Telnet (TCP port 23) and many of the Unix “r” tools, such as `rlogin`, `rsh`, `rexec`, and `rcp`. While Telnet provides plaintext remote access to a system, all SSH transmissions (both authentication and data exchange) are encrypted. SSH operates over TCP port 22. SSH is frequently used with a terminal emulator program such as Minicom or PuTTY. An example of SSH use would involve remotely connecting to a web server, firewall, switch, or router in order to make configuration changes.

SSH is a very flexible tool. It can be used as a secure Telnet replacement; it can be used to encrypt protocols (such as SFTP, SEXEC, SLOGIN, and SCP) similar to how TLS operates; and it can be used as a VPN protocol. However, as a VPN, SSH is limited to transport mode (i.e., end-to-end encryption between individual hosts, aka link encryption and host-to-host VPN). The tool OpenSSH is a means to implement SSH VPNs.

For most secure protocols, if the *S* in the name is a prefix, like with SFTP, then the encryption is provided by SSH (which has an *S* as its first letter). If the *S* in the name is a suffix, like with HTTPS, then the encryption is provided by TLS (which has S as its last letter).

OpenVPN

OpenVPN is based on TLS (formally SSL) and provides an easy-to-configure but robustly secured VPN option. OpenVPN is an open source implementation that can use either preshared passwords or certificates for authentication. Many WAPs support OpenVPN, which is a native VPN option for using a home or business WAP as a VPN gateway.

IP Security Protocol

Internet Protocol Security (IPSec) is a standard of IP security extensions used as an add-on for IPv4 and integrated into IPv6. The primary use of IPSec is for establishing VPN links between internal and/or external hosts or networks. IPSec works only on IP networks and provides for secured authentication as well as encrypted data transmission. IPSec is sometimes paired with L2TP as L2TP/IPSec.

IPSec isn't a single protocol but rather a collection of protocols, including AH, ESP, HMAC, IPComp, and IKE.

Authentication Header (AH) provides assurances of message integrity and nonrepudiation. AH also provides the primary

authentication function for IPSec, implements session access control, and prevents replay attacks.

Encapsulating Security Payload (ESP) provides confidentiality and integrity of payload contents. It provides encryption, offers limited authentication, and prevents replay attacks. Modern IPSec ESP typically uses advanced encryption standard (AES) encryption. The limited authentication allows ESP to establish its own links without using AH and perform periodic mid-session reauthentication to detect and respond to session hijacking. ESP can operate in either transport mode or tunnel mode.

Hash-based Message Authentication Code (HMAC) is the primary hashing or integrity mechanism used by IPSec.

IP Payload Compression (IPComp) is a compression tool used by IPSec to compress data prior to ESP encrypting it in order to attempt to keep up with wire-speed transmission.

IPSec uses public-key cryptography and symmetric cryptography to provide encryption (aka hybrid cryptography), secure key exchange, access control, nonrepudiation, and message authentication, all using standard Internet protocols and algorithms. The mechanism of IPSec that manages cryptography keys is *Internet Key Exchange (IKE)*. IKE is composed of three elements: OAKLEY, SKEME, and ISAKMP. OAKLEY is a key generation and exchange protocol similar to Diffie–Hellman. *Secure Key Exchange Mechanism (SKEME)* is a means to exchange keys securely, similar to a digital envelope. Modern IKE implementations may also use ECDHE for key exchange. *Internet Security Association and Key Management Protocol (ISAKMP)* is used to organize and manage the encryption keys that have been generated and exchanged by OAKLEY and SKEME. A security association is the agreed-on method of authentication and encryption used by two entities (a bit like a digital keyring). ISAKMP is used to negotiate and provide authenticated keying material (a common method of authentication) for security associations in a secured manner. Each IPSec VPN uses two security associations, one for encrypted transmission and the other for encrypted reception. Thus, each IPSec VPN is composed of two simplex communication channels that are independently encrypted.

ISAKMP's use of two security associations per VPN is what enables IPSec to support multiple simultaneous VPNs from each host.

Switching and Virtual LANs

Switches are the most common modern network management device. A switch operates primarily at Layer 2 but may be equipped to operate at Layer 3 (or higher) for specialty purposes. An unmanaged switch has no configuration options. A managed switch may offer numerous configuration options, such as VLANs and MAC limiting.

All switches operate around four primary functions: learning, forwarding, dropping, and flooding.

Learning or learning mode is how a switch becomes aware of its local network. Each received inbound Ethernet frame is evaluated. First, the source MAC address is checked against the content addressable memory (CAM) table. The CAM table is held in switch memory and contains a mapping between MAC address and port number. In this case, the port number is the physical RJ-45 jack rather than a Transport-layer protocol concern. If the Ethernet frame's source MAC address is not in the CAM table, it is added. Second, the destination MAC address is checked against the CAM table. If the address is present, then the exit port in the table is compared to the port that the current Ethernet frame was received on. If the port numbers are different, then the frame is forwarded out the exit port. If the port numbers are the same, then the frame is dropped (since it is already present on the correct network segment). If the destination MAC address is not present in the CAM table, then it is flooded or sent out all ports. This is done to hopefully allow the frame to reach its destination even if the destination is not known.

A *virtual local area network (VLAN)* is a hardware-imposed network segmentation created by switches. By default, all ports on a switch are part of VLAN 1. But as the switch administrator changes the VLAN assignment on a port-by-port basis, various ports can be grouped together and kept distinct from other VLAN port designations. VLANs can also be assigned or created based on the device's MAC address, IP subnetting, specified protocols, or

authentication. VLAN management is most commonly used to distinguish between user traffic and management traffic. VLAN 1, the default VLAN, is typically designated as the VLAN for management traffic.

VLANs are used for traffic management because they are a form of network segmentation. Network segments exist to contain traffic within and block traffic attempting to exit or enter. Communications between members of the same VLAN occur without hindrance, but communications between VLANs require a routing function. VLAN routing can be provided either by an external router or by the switch's internal software (one reason for the terms *L3 switch* and *multilayer switch*). VLANs are treated like subnets but aren't subnets. VLANs are created by switches. Subnets are created by IP address and subnet mask assignments.

VLAN management is the use of VLANs to control traffic for security or performance reasons. VLANs can be used to isolate traffic between network segments. This can be accomplished by not defining a route between different VLANs or by specifying a deny filter between certain VLANs (or certain members of a VLAN). Any network segment that doesn't need to communicate with another in order to accomplish a work task/function shouldn't be able to do so. VLANs should be used to allow communications that are necessary and to block/deny anything that isn't necessary. Remember, “deny by default; allow by exception” isn't a guideline just for firewall rules but for security in general.

VLANs are used to segment a network logically without altering its physical topology. They are easy to implement, have little administrative overhead, and are a hardware-based solution (specifically a Layer 3 switch). As networks are being crafted in virtual environments or in the cloud, software switches or virtual switches are often used. In these situations, VLANs are not hardware-based but instead are switch software–based implementations or impositions. A VLAN is an example of a virtualized network.

In cloud and virtual environments, *distributed virtual switches* are becoming more common than stand-alone virtual switches because they help reduce the chance of introducing configuration errors. They are more easily centrally managed and can be managed using an infrastructure as code (IaC) architecture approach.

VLANs control and restrict broadcast traffic and reduce a network's vulnerability to sniffers because a switch treats each VLAN as a separate network division. It's the routing function between VLANs that blocks Ethernet broadcasts between subnets and VLANs, because a router (or any device performing Layer 3 routing functions such as a Layer 3 switch) doesn't forward Layer 2 Ethernet broadcasts. This feature of a switch blocks Ethernet broadcasts between VLANs and so helps protect against broadcast storms. A *broadcast storm* is a flood of unwanted Ethernet broadcast network traffic.

Another element of some VLAN deployments is that of *port isolation* or *private ports*. These are private VLANs that are configured to use a dedicated or reserved uplink port. The members of a private VLAN or a port-isolated VLAN can interact only with each other and over the predetermined exit port or uplink port. A common implementation of port isolation occurs in hotels. A hotel network can be configured so that the Ethernet ports in each room or suite are isolated on unique VLANs. This way, connections in the same unit can communicate but connections between units cannot. However, all of these private VLANs have a path out to the Internet (i.e., the uplink port).

Switch Eavesdropping

A port mirror is a common feature found on managed switches; it will duplicate traffic from one or more other ports out a specific port. A switch may have a hardwired *Switched Port Analyzer (SPAN)* port, which duplicates the traffic for all other ports, or any port can be configured as the mirror, audit, IDS, or monitoring port for one or more other ports. Port mirroring or port spanning takes place on the switch itself. Port mirroring and spanning is often used for network traffic analysis, packet capture, evidence collection, and intrusion detection.

A *port tap* is a means to eavesdrop on network communications, especially when a switch's SPAN function isn't available or doesn't meet the current interception needs. Modern inline taps have mostly replaced vampire taps. To install an inline tap, first, the original cable must be unplugged from the port and then plugged into the tap. Then, the tap is plugged into the vacated original port. A tap should be installed wherever traffic monitoring on a specific cable is required.

If there are more devices in an area than there are ports on a switch, additional switches can be deployed. Several switches can be linked together through their trunk ports. A trunk port is a dedicated port with higher bandwidth capacity than the other standard access ports. Switches are typically linked using a crossover cable, but if the ports are Auto-MDIX (medium-dependent interface crossover), then they will automatically configure themselves to adapt to whatever cable is used to link the devices.

The trunk link allows the switches to talk to each other directly, direct traffic between hosts, and stretch VLAN definitions across multiple physical switches. In this manner, VLAN3 on switch 2 can be part of the same VLAN as VLAN3 on switches 4 and 5. This is accomplished using special signaling defined in *IEEE 802.1q* (Dot1q) known as VLAN tagging. VLAN tags modify the standard construction of an Ethernet frame header to include a VLAN tag value. A standard Ethernet header is:

```
[Dst MAC | Src MAC | Ethertype]
```

A modified Ethernet header with a VLAN tag is structured like this:

```
[Dst MAC | Src MAC | VLAN | Ethertype]
```

Thus, a VLAN tag–modified Ethernet header cannot be interpreted by any host other than a switch, and then the switch is prepared to do so only on a trunk port.

However, there is the possibility of abuse of the VLAN tag system. An attacker could construct a header with multiple tags in order to perform *VLAN hopping*. The double-tagged Ethernet frame could start off in VLAN3 but then move into VLAN2. Early switches were not prepared for double tagging, so after reading the first VLAN tag into memory (such as VLAN3), the second VLAN tag (such as VLAN2) would overwrite the first in memory, thus only retaining the second value. When the switch then began to forward the frame, it would be placed into the second VLAN group.

The concept of OS virtualization has given rise to other virtualization topics, such as virtualized networks. A virtualized network or network virtualization is the combination of hardware and software networking components into a single integrated entity. The resulting system allows for software control over all network functions: management, traffic shaping, address assignment, and so on. A single management console or interface can be used to oversee every aspect of the network, a task requiring physical presence at each hardware component in the past. Virtualized networks have become a popular means of infrastructure deployment and management by corporations worldwide. They allow organizations to implement or adapt other interesting network solutions, including software-defined networks, VLANs, virtual switches, virtual SANs, guest operating systems, port isolation, and more. Virtual networks are also discussed in Chapter 11, and software-defined networking (SDN) is discussed in Chapter 9.

MAC Flooding Attack

A *MAC flooding* attack is an intentional abuse of a switch's learning function to cause it to get stuck flooding. This is accomplished by

flooding a switch with Ethernet frames with randomized source MAC addresses. The switch will attempt to add each newly discovered source MAC address to its content addressable memory (CAM) table. Once the CAM table is full, older entries will be dropped to make room for new entries (it is a first-in, first-out [FIFO] queue). Once the CAM is full of only false addresses, the switch is unable to properly forward traffic, so it reverts to flooding mode, where it acts like a hub or a multiport repeater and sends each received Ethernet frame out of every port.

MAC flooding is distinct from ARP poisoning and other types of AitM attacks in that the attacker does not get into the path of the communication between client and server; instead, the attacker (as well as everyone else on the local network) gets a copy of the communication. At this point, the attacker can eavesdrop on any communications taking place across the compromised switch.

A defense against MAC flooding is often present on managed switches. The feature, known as *MAC limiting*, restricts the number of MAC addresses that will be accepted into the CAM table from each jack/port. A network intrusion detection system (NIDS) may also be useful in identifying when a MAC flooding attack is attempted.

MAC Cloning

No two devices can have the same MAC address in the same local Ethernet broadcast domain; otherwise, an address conflict occurs. It is also good practice to verify that all MAC addresses across a private enterprise network are unique. This can be accomplished through manual NIC configuration checks as well as by remote queries performed by network discovery scanners. Although the design of MAC addresses should make them unique, vendor errors have produced duplicate MAC addresses. When this happens, either the NIC hardware must be replaced, or the MAC address must be modified (i.e., spoofed) to a nonconflicting alternative address.

An adversary may eavesdrop on a network and take note of the MAC addresses in use. One of these addresses can then be spoofed into a system by altering the system's software copy of the NIC's MAC. This causes the Ethernet driver to operate based on the modified or spoofed MAC address instead of the original manufacturer's assigned

MAC. Thus, it is quite simple to falsify, spoof, or clone a MAC address.

MAC spoofing is the changing of the default MAC address to some other value. *MAC cloning* is used to impersonate another system, often a valid or authorized network device, to bypass port security or MAC filtering limitations. *MAC filtering* is a security mechanism intended to limit or restrict network access to those devices with known specific MAC addresses. MAC filtering is commonly used on WAPs and switches.

Countermeasures to MAC spoofing/cloning include the following:

- Using intelligent switches that monitor for odd MAC address uses and abuses
- Using an NIDS that monitors for odd MAC address uses and abuses
- Maintaining an inventory of devices and their MAC addresses to confirm whether a device is authorized or unknown and rogue

To spoof a MAC address on *nix systems, you can use the utility `macchanger`. On Windows, use the free tools of Technitium from http://technitium.com/tmac or the SMAC Tool from http://smac-tool.com.

Network Address Translation

The goals of hiding the identity of internal clients, masking the design of your private network, and keeping public IPv4 address leasing costs to a minimum are all simple to achieve through the use of *network address translation (NAT)*. NAT hides the IPv4 configuration of internal clients and substitutes the IPv4 configuration of the proxy server's own public external NIC in outbound requests. This effectively prevents external hosts from learning the internal configuration of the network. This is an

essential function when using RFC 1918 (Address Allocation for Private Internets) private IPv4 addresses internally while communicating with Internet resources.

NAT was developed to allow private networks to use any IPv4 address set without causing collisions or conflicts with public Internet hosts with the same IPv4 addresses. In effect, NAT translates the IPv4 addresses of your internal clients to leased addresses outside your environment. Functionally, NAT is a form of virtualized network; it hides or masks the real network configuration behind its own public identity.

NAT offers numerous benefits, including the following:

- You can connect an entire network to the Internet using only a single (or just a few) leased public IPv4 addresses.
- You can use the private IPv4 addresses defined in RFC 1918 in a private network and still be able to communicate with the Internet.
- NAT hides the IPv4 addressing scheme and network topography from the Internet.
- NAT restricts connections so that only traffic stemming from connections originating from the internal protected network is allowed back into the network from the Internet. Thus, most intrusion attacks are automatically repelled.
- NAT serves as a basic one-way firewall by only allowing incoming traffic that is in response to an internal system's request.

Are You Using NAT?

Most networks, whether at an office or at home, employ NAT. There are at least three ways to tell whether you are working within a "NATed" network:

- Check your client's IPv4 address. If it is one of the RFC 1918 addresses and you are still able to interact with the Internet, then you are on a NATed network.
- Check the configuration of your proxy, router, firewall, modem, or gateway device to see whether NAT is configured. (This action requires authority and access to the networking device.)
- If your client's IPv4 address is not an RFC 1918 address, then compare your address to what the Internet thinks your address is. You can do this by visiting any of the IP-checking websites; a popular one is http://whatismyipaddress.com. If your client's IPv4 address and the address that What Is My IP Address claims is your address are different, then you are working from a NATed network.

NAT is part of a number of hardware devices and software products, including firewalls, routers, gateways, WAPs, and proxies.

Strictly, NAT dynamically converts or maps the private IPv4 addresses of internal systems found in the header of network packets into public or external IPv4 addresses. NAT performs this operation on a one-to-one basis; thus, a single leased public IPv4 address can allow a single internal system to access the Internet. Closely related to NAT is *port address translation (PAT)*—also known as *overloaded NAT*, *network and port address translation (NPAT)*, and *network address port translation (NAPT)*—which allows a single public IPv4 address to host up to 65,536 simultaneous communications from internal clients (a theoretical maximum; in practice, you should limit the number to 4,000 or fewer in most cases due to hardware limitations). Instead of mapping IPv4 addresses on a one-to-one

basis, PAT uses the Transport Layer port numbers to host multiple simultaneous communications across each public IPv4 address by mapping internal sockets (i.e., the combination of an IPv4 address and a port number) to external sockets. PAT is effectively multiplexing numerous sessions from internal systems over a single external IPv4 address. So, with NAT, you must lease as many public IPv4 addresses as you want to have simultaneous communications, whereas with PAT you can lease significantly fewer IPv4 addresses.

The use of the term NAT in the IT industry has come to include the concept of PAT. Thus, when you hear or read about NAT, you can assume that the material is referring to PAT. This is true for most OSs, devices, and services. *Source Network Address Translation (SNAT)* is yet another term for NAT. NAT can also be called Stateful NAT or Dynamic NAT since the mapping and IPv4 address or socket allocation is created when a session is initiated and dissolved when the session is torn down (see the section “Stateful NAT,” later in this chapter). From this point forward, our use of the term NAT is meant to imply the more likely use of PAT.

Another issue to be familiar with is that of *NAT traversal (NAT-T)* (RFC 3947). Traditional NAT doesn't support IPSec VPNs, because of the requirements of the IPSec protocol and the changes NAT makes to packet headers (which is perceived as corruption or violating integrity). However, NAT-T was designed specifically to support IPSec and other tunneling VPN protocols, such as Layer 2 Tunneling Protocol (L2TP), so that organizations can benefit from both NAT and VPNs across the same border device/interface.

Although NAT by default is a dynamic outbound mapping mechanism, it can be configured to perform inbound mapping as well. Known as *static NAT*, *reverse proxy*, *port forwarding*, or *destination network address translation (DNAT)*, this technique allows an external entity to initiate communication with an internal entity behind a NAT by using a public socket that is mapped to redirect to an internal system's private address. Though this is technically possible, it is generally to be avoided. Granting the easy ability for an external entity to initiate a connection with an internal system is not usually a secure solution. Static NAT may be useful for

systems in a screened subnet or extranet, but definitely not for accessing systems in the internal private LAN.

NAT66, or Network Address Translation for IPv6, is a technique used to map multiple private IPv6 addresses to a smaller pool of public IPv6 addresses. The primary goal of NAT66 is similar to traditional NAT used in IPv4 networks, which is to enable multiple devices within a private network to share a single or a limited set of globally routable IPv6 addresses.

NAT66 allows multiple devices within a private IPv6 network to share the same public IPv6 address when communicating with external networks, such as the Internet. NAT66 provides a level of privacy and security by hiding internal network details from external entities. It assigns global IPv6 addresses to devices within the private network, and external entities see only the public IPv6 address. Although IPv6 has a vastly larger address space compared to IPv4, there may still be scenarios where organizations want to conserve public IPv6 addresses. NAT66 can be used to achieve this goal by allowing multiple internal devices to share a common public IPv6 address.

It's important to note that while NAT66 is an option, IPv6 was originally designed with the goal of providing globally unique addresses to all devices, promoting end-to-end connectivity without the need for address translation. The use of NAT in IPv6 has been a topic of debate, and some advocate for maintaining the original design principles of IPv6. However, in certain deployment scenarios or due to specific network requirements, organizations may choose to implement NAT66 for address conservation and security purposes.

Private IP Addresses

The world has simply deployed more devices using IPv4 than there are unique IPv4 addresses available. Fortunately, the early designers of the Internet and TCP/IP had good foresight and put aside a few blocks of addresses for private, unrestricted use. These IPv4 addresses, commonly called the *private IPv4 addresses*, are defined in *RFC 1918*. They are as follows:

- 10.0.0.0–10.255.255.255 (a full Class A range)
- 172.16.0.0–172.31.255.255 (16 Class B ranges)
- 192.168.0.0–192.168.255.255 (256 Class C ranges)

Can't NAT Again

On several occasions we've needed to "re-NAT" an already "NATed" network. This might occur in the following situations:

- You need to make an isolated subnet within a NATed network and attempt to do so by connecting a router to host your new subnet to the single port offered by the existing network.
- You have a DSL or cable modem that offers only a single connection but you have multiple computers or want to add wireless to your environment.

By connecting a NAT proxy router or a wireless access point, you are usually attempting to re-NAT what was NATed to you initially. One configuration setting that can either make or break this setup is the IPv4 address range in use. It is not possible to re-NAT the same subnet. For example, if your existing network is offering 192.168.1.x addresses, then you cannot use that same address range in your new NATed subnet. So change the configuration of your new router/WAP to perform NAT on a slightly different address range, such as 192.168.5.x, and you won't have the conflict. This seems obvious, but it is quite frustrating to troubleshoot the unwanted result without this insight.

All routers and traffic-directing devices are configured by default not to forward traffic to or from these private IPv4 addresses. In other words, the private IPv4 addresses are not routed by default. Thus, they cannot be directly used to communicate over the Internet. However, they can be easily used on private networks where routers are not employed or where slight modifications to router

configurations are made. Using private IPv4 addresses in conjunction with NAT greatly reduces the cost of connecting to the Internet by allowing fewer public IPv4 addresses to be leased from an ISP.

Attempting to use the RFC 1918 private IPv4 addresses directly on the Internet is futile because all publicly accessible routers will drop data packets containing a source IPv4 address from these RFC 1918 ranges.

Stateful NAT

NAT operates by maintaining a mapping between requests made by internal clients, a client's internal IP address, and the IP address of the Internet service contacted. When a request packet is received by NAT from a client, it changes the source address in the packet from the client's to the NAT server's. This change is recorded in the NAT mapping database along with the destination address. Once a reply is received from the Internet server, NAT matches the reply's source address to an address stored in its mapping database and then uses the linked client address to redirect the response packet to its intended destination. This process is known as *stateful NAT* because it maintains information about the communication sessions between clients and external systems.

Automatic Private IP Addressing

Automatic Private IP Addressing (APIPA), also known as IPv4 link-local address assignment (defined in RFC 3927), assigns an IP address to a system in the event of a Dynamic Host Configuration Protocol (DHCP) assignment failure. APIPA is primarily a feature of Windows, since no other OS has adopted the standard. APIPA assigns each failed DHCP client an IP address from the range of 169.254.0.1 to 169.254.255.254, along with the default Class B subnet mask of 255.255.0.0. This allows the system to communicate only with other APIPA-configured clients within the same broadcast

domain but not with any system across a router or with a correctly assigned IP address.

Don't confuse APIPA with the private IP address ranges defined in RFC 1918.

APIPA is not usually directly concerned with security. However, it is still an important issue to understand. If you notice that a system is assigned an APIPA address instead of a valid network address, that indicates a problem. It could be as mundane as a bad cable or power failure on the DHCP server, but it could also be a symptom of a malicious attack on the DHCP server. You might be asked to decipher issues in a scenario where IP addresses are presented. You should be able to discern whether an address is a public address, an RFC 1918 private address, an APIPA address, or a loopback address (see Chapter 11).

The Loopback Address

Another IP address range that you should be careful not to confuse with the private IP address ranges defined in RFC 1918 is the loopback address. The *loopback address* is purely a software entity. It is an IP address used to create a software interface that connects back to itself via TCP/IP. The loopback address allows for the testing of local network settings in spite of missing, damaged, or nonfunctional network hardware and related device drivers. Technically, the entire 127.x.x.x network is reserved for loopback use. However, only the 127.0.0.1 address is widely used.

Third-Party Connectivity

Third-party connectivity is a growing concern for almost every business. Very few organizations operate exclusively using internal resources—most organizations interact with outside third-party providers. Most of these external entities do not need to interact

directly with an organization's IT/IS. However, for those few that do, it is important to consider the risks and ramifications. Any time an organizational network is connected directly to another entity's network, their local threats and risks affect each other. A compromise of one organization can lead easily to the compromise of the other.

Any connection between IT environments should be planned out in detail well in advance of actually interconnecting the cabling (whether physical or virtual). Often, this process starts with an MOU and ends with an ISA:

- A *memorandum of understanding (MOU)* or memorandum of agreement (MOA) is an expression of agreement or aligned intent, will, or purpose between two entities. It is not typically a legal agreement or commitment, but rather a more formal form of a reciprocal agreement or handshake (neither of which is typically written down). An MOU can also be called a letter of intent. It is a means to document the specifics of an agreement or arrangement between two parties without necessarily legally binding them to the parameters of the document.
- An *interconnection security agreement (ISA)* is a formal declaration of the security stance, risks, and technical requirements of a link between two organizations' IT infrastructures. The goal of an ISA is to define the expectations and responsibilities of maintaining security over a communications path between two networks. Connecting networks can be mutually beneficial, but it also raises additional risks that need to be identified and addressed. An ISA is a means to accomplish that.

Additionally, a full risk assessment should be performed in order to predict issues and preemptively protect against adverse events as much as possible.

Keep in mind that direct linking of IT environments is not the only possible solution in most circumstances. Using an extranet to host servers to be accessed by the other party via a VPN is a reasonable alternative. Another option is to work with a cloud solution to establish a shared private cloud between the two entities so that only

project-related content is ever shared between the two parties. A third option is to keep all datasets separate and use secure email, file sharing, and multimedia collaboration services.

Whatever approach you decide to use, don't let the rush or haste of establishing a new relationship with a third party or engaging in a new project cause security to be discarded or overlooked.

Similar care should be taken when electing to use a cloud service, since they are third parties. As an organization adopts cloud services, from SaaS to IaaS, the level of connectivity and direct interaction with on-premises equipment increases. Clear security guidelines and policies should be established, and when possible, technologies such as cloud access security brokers (CASBs) should be deployed to enforce those security requirements.

Yet another possible interpretation of third-party connectivity is a remote worker or telecommuter. As mentioned previously, there needs to be clear justification for allowing remote work, which requires a direct link or access to internal resources. When possible, limit telecommuters to extranet servers or only publicly facing systems (such as email and websites). It may also be important to provide company-owned and -controlled equipment to remote workers rather than depending on personal equipment, which may not be securable or may be used for nonwork purposes or by nonemployees.

Third-party connectivity is a risk that can be managed, but it requires focused and purposed attention. Remember that any means of data transmission or communication can be employed by benign actors for legitimate purposes as well as by adversaries for malicious purposes.

WAN technologies are critical for establishing connectivity over large geographical areas. In the context of third-party connectivity involving telecom providers and hardware support, several key considerations come into play. Telecom providers play a central role in WAN connectivity, offering services like leased lines, Multiprotocol Label Switching (MPLS), and virtual private network (VPN) services. Leased lines provide dedicated point-to-point connections, whereas MPLS and VPN services enable secure and efficient data transmission over shared infrastructure.

Hardware support is equally vital in WAN connectivity, involving components such as routers, switches, and WAN optimization appliances. These devices are essential for establishing and managing WAN connections. Hardware support ensures proper functioning, maintenance, and troubleshooting, either through internal IT teams or third-party vendors specializing in networking hardware.

MPLS services are commonly employed in WAN connectivity, providing businesses with the means to create private and secure networks across multiple locations. MPLS incorporates quality of service (QoS) features, addressing specific performance requirements. With the rise of cloud services, WAN technologies play a pivotal role in connecting organizations to cloud providers. Telecom providers offer solutions facilitating direct connections to major cloud platforms, enhancing performance, security, and reliability for cloud-based applications.

Software-defined WAN (SD-WAN) is a modern approach to WAN connectivity that utilizes software-defined networking principles. It allows organizations to dynamically route traffic over various connections, optimizing performance and cost-effectiveness. Telecom providers may offer SD-WAN services to enhance network flexibility and efficiency.

Redundancy and failover mechanisms are crucial components of WAN technologies to ensure continuous connectivity. This may involve the use of multiple telecom providers or diverse network paths to minimize the risk of service disruption. Hardware support is essential for maintaining and configuring these redundant setups.

WAN technologies in the context of third-party connectivity involve collaboration with telecom providers and the utilization of hardware components. Organizations leverage a mix of technologies, including leased lines, MPLS, VPNs, SD-WAN, and others, to establish efficient and reliable connectivity across diverse locations. Hardware support, whether provided internally or by third-party vendors, is essential for maintaining the integrity and performance of the WAN infrastructure. The choice of WAN technologies and third-party partnerships depends on factors such as performance requirements, cost considerations, and the specific needs of the organization.

Switching Technologies

When two systems (individual computers or LANs) are connected over multiple intermediary networks, the task of transmitting data from one to the other is a complex process. Switching technologies were developed to simplify this task.

Circuit Switching

Circuit switching was originally developed to manage telephone calls over the public switched telephone network. In circuit switching, a dedicated physical pathway is created between the two communicating parties. Once a call is established, the links between the two parties remain the same throughout the conversation. Circuit switching provides for fixed or known transmission times, a uniform level of quality, and little or no loss of signal or communication interruptions. These systems employ permanent, physical connections. However, the term permanent applies only to each communication session. The path is permanent throughout a single conversation. Once the path is disconnected, if the two parties communicate again, a different path may be assembled. During a single conversation, the same physical or electronic path is used throughout the communication and is used only for that one communication. Circuit switching grants exclusive use of a communication path to the current communication partners. Only after a session has been closed can a pathway be reused by another communication.

Real-World Circuit Switching

There is very little actual circuit switching in the modern world (or at least in the past 20 to 25 years or so). Packet switching, discussed next, has become ubiquitous for data and voice transmissions. Decades ago, we could often point to the public switched telephone network (PSTN) as a prime example of circuit switching, but with the advent of digital switching and VoIP systems, those days are long gone. That's not to say that circuit switching is nonexistent in today's world; it is just not being used for data transmission. Instead, you can still find circuit switching in rail yards, irrigation systems, and even electrical distribution systems.

Packet Switching

Eventually, as computer communications increased as opposed to traditional voice communications, a new form of switching was developed. *Packet switching* occurs when the message or communication is broken up into small segments (fixed-length cell or variable-length packets, depending on the protocols and technologies employed) and sent across the intermediary networks to the destination. Each segment of data has its own header that contains source and destination information. The header is read by each intermediary system and is used to route each packet to its intended destination. Each channel or communication path is reserved for use only while a packet is actually being transmitted over it. As soon as the packet is sent, the channel is made available for other communications.

Packet switching does not enforce the exclusivity of communication pathways. It can be seen as a logical transmission technology because addressing logic dictates how communications traverse intermediary networks between communication partners. Table 12.2 compares circuit switching to packet switching.

TABLE 12.2 Circuit switching vs. packet switching

Circuit switching	Packet switching
Constant traffic	Bursty traffic
Fixed known delays	Variable delays
Connection-oriented	Connectionless
Sensitive to connection loss	Sensitive to data loss
Used primarily for voice	Used for any type of traffic

In relation to security, you should consider a few potential issues. A packet-switching system places data from different sources on the same physical connection. This can lend itself to disclosure, corruption, or eavesdropping. Proper connection management, traffic isolation, and usually encryption are needed to protect against shared physical pathway concerns. A benefit of packet-switching networks is that they are not as dependent on specific physical connections as circuit switching is. Thus, when or if a physical pathway is damaged or goes offline, an alternate path can be used to continue the data/packet delivery. A circuit-switching network is often interrupted by physical path violations.

Virtual Circuits

A *virtual circuit* (also called a communication path) is a logical pathway or circuit created over a packet-switched network between two specific endpoints. Within packet-switching systems are two types of virtual circuits:

- *Permanent virtual circuits (PVCs)*
- *Switched virtual circuits (SVCs)*

A PVC is like a dedicated leased line; the logical circuit always exists and is waiting for the customer to send data. A PVC is a predefined virtual circuit that is always available. The virtual circuit may be closed down when not in use, but it can be instantly reopened whenever needed. An SVC has to be created each time it is needed using the best paths currently available before it can be used and then disassembled after the transmission is complete. In either type

of virtual circuit, when a data packet enters point A of a virtual circuit connection, that packet is sent directly to point B or the other end of the virtual circuit. However, the actual path of one packet may be different from the path of another packet from the same transmission. In other words, multiple paths may exist between point A and point B as the ends of the virtual circuit, but any packet entering at point A will end up at point B.

A PVC is like a two-way radio or walkie-talkie. Whenever communication is needed, you press the button and start talking; the radio reopens the predefined frequency automatically (that is, the virtual circuit). An SVC is more like a shortwave or ham radio. You must tune the transmitter and receiver to a new frequency every time you want to communicate with someone.

WAN Technologies

WAN technologies contribute to the efficiency, scalability, and reliability of long-distance communications. The selection of a specific technology hinges on factors such as geographical locations, bandwidth requirements, latency sensitivity, and the unique needs of the applications being supported. Each technology plays a role in addressing connectivity challenges across diverse and often remote environments.

Wide area network links are used to connect distant networks, nodes, or individual devices together. A WAN link can improve communications and efficiency, but it can also place data at risk. Proper connection management and transmission encryption is needed for a secure connection, especially over public network links. WAN links and long-distance connection technologies can be divided into two primary categories: dedicated and nondedicated.

A *dedicated line* (also called a *leased line* or *point-to-point link*) is one that is continually reserved for use by a specific customer. A dedicated line is always on and waiting for traffic to be transmitted over it. The link between the customer's LAN and the dedicated WAN link is always open and established. A dedicated line connects two specific endpoints and only those two endpoints. This type of

connection is often used between multiple business locations, so they can effectively communicate as a single entity.

There have been numerous types of dedicated lines over the years, ranging from the T1 (telephone line 1 with 1.54 Mbps capacity) to DS3 (Digital Service 3 with 44.7 Mbps capacity) (originally known as the T3). Other options included X.25, Asynchronous Transfer Mode (ATM), and Frame Relay. These technologies have mostly been replaced by fiber optic–based solutions.

Cable TV–based Internet service does not fit well into either the dedicated or the nondedicated classification. Cable Internet is an always-on system, but not between two client locations. Instead, it is a link from your premises to an Internet gateway. Thus, it can be labeled as a point-to-multipoint connection. Another wrinkle is that cable Internet service is also typically shared with the other subscribers in the neighborhood. Privacy is maintained through encryption, similar to a VPN, from the cable modem deployed at your location to an exit point in the cable company's network, typically immediately connected to the Internet gateway.

A *nondedicated line* is one that requires a connection to be established before data transmission can occur. A nondedicated line can be used to connect with any remote system that uses the same type of nondedicated line.

Fault Tolerance with Carrier Network Connections

To obtain fault tolerance with leased lines or with connections to carrier networks, you must deploy two redundant connections. For even greater redundancy, you should purchase the connections from two different telcos or service providers. However, when you're using two different service providers, be sure they don't connect to the same regional backbone or share any major pipeline. The physical location of multiple communication lines leading from your building is also of concern because a single disaster or human error (e.g., a misguided backhoe) could cause multiple lines to fail at once. If you cannot afford to deploy an exact duplicate of your primary dedicated leased line, consider a nondedicated connection. These less expensive options may still provide partial availability in the event of a primary leased line failure.

Standard classic dial-up modems and DSL modems are examples of nondedicated lines. Digital subscriber line (DSL) is a technology that exploits the upgraded telephone network to grant consumers speeds from 144 Kbps to 100 Mbps (or more). There are numerous formats of DSL (e.g., ASDL, VSDL, and SDSL), and each format varies according to the specific downstream and upstream bandwidth provided.

Backhaul networks constitute the segment linking smaller or local networks to a central hub or the broader Internet. Various WAN technologies are applied in this context to ensure effective connectivity. MPLS (Multiprotocol Label Switching) stands out as a prevalent choice, offering scalability and efficiency by utilizing labels for packet routing. This approach is conducive to connecting diverse locations and supporting quality of service (QoS) features. Additionally, Ethernet-based solutions, such as Metro Ethernet, are commonly employed in backhaul connections, providing high bandwidth, scalability, and flexibility for applications spanning cell towers, business locations, and data centers.

Satellite communications involve the transmission of data between Earth-based stations or satellite-enabled devices, relying on satellites orbiting Earth. In this domain, very-small-aperture terminal (VSAT) technology plays a pivotal role. VSAT enables small, remote terminals to communicate with geostationary satellites, proving useful in locations where traditional wired or terrestrial connections pose challenges. Satellite broadband services leverage satellites to extend Internet connectivity to remote or underserved areas. Users with satellite dishes can establish connections, facilitating broadband access where terrestrial options may be limited. Moreover, the emergence of low Earth orbit (LEO) satellites, exemplified by projects like Starlink, offers a contemporary approach to satellite communications with reduced latency compared to traditional geostationary satellites. LEO satellites aim to provide high-speed Internet access globally.

Broadband over power lines (BPL) is a technology that enables high-speed data transmission over existing electrical power lines. In a BPL system, data signals are transmitted along the same infrastructure that is used to deliver electric power. This technology leverages the extensive network of power lines to provide broadband Internet access to homes, businesses, and other locations. While BPL has been explored as a potential solution for extending broadband access, its adoption has been limited compared to other technologies like DSL, cable, and fiber optics. Factors such as technical challenges, regulatory considerations, and the growth of alternative broadband technologies have influenced the deployment and acceptance of BPL in different regions.

Integrated Services Digital Network (ISDN) was the planned replacement for PSTN, but with the advent of DSL, cable Internet, and fiber options, it did not gain widespread adoption. Most ISDN services have been discontinued.

Fiber-Optic Links

Synchronous Digital Hierarchy (SDH) and *Synchronous Optical Network (SONET)* are fiber-optic high-speed networking standards. SDH was standardized by the International Telecommunications Union (ITU) and SONET by the American National Standards Institute (ANSI). SDH and SONET are mostly hardware or physical layer standards defining infrastructure and line speed requirements. SDH and SONET use synchronous time-division multiplexing (TDM) for high-speed duplex communications with minimal need for control and management overhead.

While SDH and SONET have some regional differences in their standards, they are functionally similar and are often used interchangeably or in conjunction with each other, particularly in international networks. *STS (Synchronous Transport Signal)* (or *Optical Carrier (OC)*) is associated with SONET, while *STM (Synchronous Transport Module)* is associated with SDH. Both STS and STM represent standardized levels within their respective hierarchies for organizing and multiplexing digital signals. These optical transmission services support a foundational speed of 51.48 Mbps. The main bandwidth levels of SDH and SONET are shown in Table 12.3.

TABLE 12.3 Bandwidth levels of SDH and SONET

SONET	SDH	Data rate
STS-1/OC-1	STM-0	51.84 Mbps
STS-3/OC-3	STM-1	155.52 Mbps
STS-12/OC-12	STM-4	622.08 Mbps
STS-48/OC-48	STM-16	2.488 Gbps
STS-96/OC-96	STM-32	4.876 Gbps
STS-192/OC-192	STM-64	9.953 Gbps
STS-768/OC-768	STM-256	39.813 Gbps

Note: The SDH service numbers are 1/3 that of SONET's.

SDH and SONET both support mesh and ring topologies. These fiber solutions are often implemented as the backbone of a telco service,

and divisions or fractions of the capacity are subscribed out to customers.

Prevent or Mitigate Network Attacks

Communication systems are vulnerable to attacks in much the same way any other aspect of the IT infrastructure is vulnerable. Understanding the threats and possible countermeasures is an important part of securing an environment. Any activity or condition that can cause harm to data, resources, or personnel must be addressed and mitigated if possible. Keep in mind that harm includes more than just destruction or damage; it also includes disclosure, access delay, denial of access, fraud, resource waste, resource abuse, and loss. Common threats against communication system security include DoS (see Chapter 17, "Preventing and Responding to Incidents"), impersonation (see Chapter 2), replay (see Chapter 11), ARP poisoning (see Chapter 11), DNS poisoning (see Chapter 11), eavesdropping, and transmission modification.

Eavesdropping

As the name suggests, *eavesdropping* is listening to communication traffic for the purpose of duplicating it. The duplication can take the form of recording data to a storage device or using an extraction program that dynamically attempts to extract the original content from the traffic stream. Once a copy of traffic content is in the hands of an attacker, they can often extract many forms of confidential information, such as usernames, passwords, process procedures, and data.

Eavesdropping usually requires physical access to the IT infrastructure to connect a physical recording device to an open port or cable splice or to install a software-recording tool onto the system. Eavesdropping is often facilitated by the use of a network traffic capture or monitoring program or a protocol analyzer system (often called a sniffer). Eavesdropping devices and software are usually difficult to detect because they are used in passive attacks. When eavesdropping or wiretapping is transformed into altering or injecting communications, the attack is considered an active attack.

You can combat eavesdropping by maintaining physical access security to prevent unauthorized personnel from accessing your IT infrastructure. As for protecting communications that occur outside your network or for protecting against internal attackers, using encryption (such as IPSec or SSH) and onetime authentication methods (onetime pads or token devices) on communication traffic will greatly reduce the effectiveness and timeliness of eavesdropping. Application allow listings should also be considered as a means to prevent the execution of unauthorized software, such as sniffers.

Modification Attacks

In *modification attacks*, captured packets are altered and then played against a system. Modified packets are designed to bypass the restrictions of improved authentication mechanisms and session sequencing. Countermeasures to modification replay attacks include using digital signature verifications and packet checksum verification (i.e., integrity checking).

Summary

Transmission Control Protocol/Internet Protocol (TCP/IP) is the primary protocol suite used on most networks and on the Internet. It is a robust protocol suite, but it has numerous security deficiencies. Authentication and encryption need to be implemented to account for TCP/IP's deficiencies.

When securing communication channels, be sure to address voice, remote access, multimedia collaboration, data communications (such as email), and virtualized networks.

Secure voice communications can be achieved by evaluating and hardening PSTN, PBX, mobile, and VoIP solutions. VoIP security is often achieved through general network security practices and using Secure Real-time Transport Protocol (SRTP).

Remote access security management requires security system designers to address the hardware and software components of the implementation along with policy issues, work task issues, and encryption issues. This includes deployment of secure

communication protocols. Secure authentication for both local and remote connections is an important foundational element of overall security.

Maintaining control over communication pathways is essential to supporting confidentiality, integrity, and availability for network, voice, and other forms of communication. Numerous attacks are focused on intercepting, blocking, or otherwise interfering with the transfer of data from one location to another. Fortunately, there are also reasonable countermeasures to reduce or even eliminate many of these threats.

VPNs are a common means to achieve data communications security. VPNs are based on encrypted tunneling. Tunneling, or encapsulation, is a means by which messages in one protocol can be transported over another network or communications system using a second protocol. VPN solutions include IPSec, TLS, SSH, L2TP, and PPTP.

Telecommuting, or remote connectivity, has become a common feature of business computing. When remote access capabilities are deployed in any environment, security must be considered and implemented to provide protection for your private network against remote access complications. Remote access users should be stringently authenticated before being granted access. Remote access services include Voice over IP (VoIP), application streaming, VDI, multimedia collaboration, and instant messaging.

Email is insecure unless you take steps to secure it. To secure email, you should provide for nonrepudiation, restrict access to authorized users, make sure integrity is maintained, authenticate the message source, verify delivery, and classify sensitive content. These issues must be addressed in a security policy before they can be implemented in a solution. They often take the form of acceptable use policies, access controls, privacy declarations, email management procedures, and backup and retention policies.

Email is a common delivery mechanism for malicious code. Filtering attachments, using antivirus software, and educating users are effective countermeasures against that kind of attack. Email spamming or flooding is a form of denial of service that can be

deterred through filters and IDSs. Email security can be improved using S/MIME and PGP.

Fax and voice security can be improved by using encryption to protect the transmission of documents and prevent eavesdropping. Training users effectively is a useful countermeasure against social engineering attacks.

Virtual networks are software or digital re-creations of physical concepts in order to achieve security or performance improvements. Examples of virtual networks include software-defined networks (SDNs), VPNs, VLANs, virtual switches, virtual SANs, guest operating systems, port isolation, and NAT.

A VLAN is a hardware-imposed network segmentation created by switches. VLANs are used to logically segment a network without altering its physical topology. VLANs are used for traffic management.

NAT is used to hide the internal structure of a private network as well as to enable multiple internal clients to gain Internet access through a few public IP addresses.

Third-party connectivity is a growing concern for businesses. Thus, it is important to consider the risks and ramifications. Any time an organizational network is connected directly to another entity's network, their local threats and risks affect each other. A compromise of one organization can lead easily to the compromise of the other. Any connection between IT environments should be planned out in detail well in advance of actually interconnecting the cabling (whether physical or virtual). Often, this process starts with an MOU and ends with an ISA.

WAN links, or long-distance connection technologies, can be divided into two primary categories: dedicated and nondedicated lines. A dedicated line connects two specific endpoints and only those two endpoints. A nondedicated line is one that requires a connection to be established before data transmission can occur.

Communication systems are vulnerable to many attacks, including distributed denial-of-service (DDoS), eavesdropping, impersonation, replay, modification, spoofing, and ARP and DNS attacks. Fortunately, effective countermeasures exist for each of these.

Study Essentials

Understand PPP. Point-to-Point Protocol (PPP) is an encapsulation protocol designed to support the transmission of IP traffic over dial-up or point-to-point links. The original PPP options for authentication were PAP, CHAP, and EAP.

Define PAP, CHAP, and EAP. Password Authentication Protocol (PAP) transmits usernames and passwords in cleartext. Challenge Handshake Authentication Protocol (CHAP) performs authentication using a challenge-response dialogue that cannot be replayed. Extensible Authentication Protocol (EAP) allows customized authentication security solutions.

Understand IEEE 802.1X. IEEE 802.1X defines the use of encapsulated EAP to support a wide range of authentication options for LAN connections. The IEEE 802.1X standard is formally named "Port-Based Network Access Control."

Know about port security. Port security can mean the physical control of all connection points, such as RJ-45 wall jacks or device ports. Port security is the management of TCP and User Datagram Protocol (UDP) ports. Port security can also refer to the need to authenticate to a port before being allowed to communicate through or across the port (i.e., IEEE 802.1X).

Understand voice communications security. Voice communications are vulnerable to many attacks, especially as voice communications become an important part of network services. You can obtain confidentiality by using encrypted communications. Countermeasures must be deployed to protect against interception, eavesdropping, tapping, and other types of exploitation.

Know the threats associated with PBX systems and the countermeasures to PBX fraud. Countermeasures to PBX fraud and abuse include many of the same precautions you would employ to protect a typical computer network: logical or technical controls, administrative controls, and physical controls.

Understand the security issues related to VoIP. VoIP is at risk for caller ID spoofing, vishing, call manager software/firmware

attacks, phone hardware attacks, DoS, AitM/MitM/on-path attacks, spoofing, and switch hopping.

Recognize what phreaking is. Phreaking is a specific type of attack in which various types of technology are used to circumvent the telephone system to make free long-distance calls, to alter the function of telephone service, to steal specialized services, or to cause service disruptions. A phreaker is an attacker who performs phreaking.

Understand the issues of remote access security management. Remote access security management requires that security system designers address the hardware and software components of an implementation along with issues related to policy, work tasks, and encryption.

Know various issues related to remote access security. Be familiar with remote access, dial-up connections, screen scrapers, virtual applications/desktops, and general telecommuting security concerns.

Understand multimedia collaboration. Multimedia collaboration is the use of various multimedia-supporting communication solutions to enhance distance collaboration and communications.

Know the purpose of load balancers. The purpose of load balancing is to obtain more optimal infrastructure utilization, minimize response time, maximize throughput, reduce overloading, and eliminate bottlenecks. A load balancer is used to spread or distribute network traffic load across several network links or network devices.

Understand active/active. An active-active system is a form of load balancing that uses all available pathways or systems during normal operations but that has reduced capacity in adverse conditions.

Understand active/passive. An active-passive system is a form of load balancing that keeps some pathways or systems in an unused dormant state during normal operations. It is able to maintain consistent capacity during abnormal conditions.

Understand virtualized networks. A virtualized network or network virtualization is the combination of hardware and software networking components into a single integrated entity. Examples include software-defined networks (SDNs), VLANs, VPNs, virtual switches, virtual SANs, guest operating systems, port isolation, and NAT.

Define tunneling. Tunneling is the encapsulation of a protocol-deliverable message within a second protocol. The second protocol often performs encryption to protect the message contents.

Understand VPNs. VPNs are based on encrypted tunneling. They can offer authentication and data protection as a point-to-point solution. Common VPN protocols are PPTP, L2TP, SSH, TLS, and IPSec.

Understand split vs. full tunnel. A split tunnel is a VPN configuration that allows a VPN-connected client system (i.e., remote node) to access both the organizational network over the VPN and the Internet directly at the same time. A full tunnel is a VPN configuration in which all of the client's traffic is sent to the organizational network over the VPN link, and then any Internet-destined traffic is routed out of the organizational network's proxy or firewall interface to the Internet.

Be able to explain NAT. NAT protects the addressing scheme of a private network, allows the use of the private IP addresses, and enables multiple internal clients to obtain Internet access through a few public IP addresses. NAT is supported by many security border devices, such as firewalls, routers, gateways, WAPs, and proxies.

Know about third-party connectivity. Most organizations interact with outside third-party providers. Most of these external entities do not need to interact directly with an organization's IT/IS. However, for those few that do, it is important to consider the risks and ramifications. This includes partnerships, cloud services, and remote workers.

Understand the difference between packet switching and circuit switching. In circuit switching, a dedicated physical pathway is created between the two communicating parties. Packet switching occurs when the message or communication is broken up

into small segments and sent across the intermediary networks to the destination. Within packet-switching systems are two types of communication paths, or virtual circuits: permanent virtual circuits (PVCs) and switched virtual circuits (SVCs).

Understand the various network attacks and countermeasures associated with communications security. Communication systems are vulnerable to many attacks, including distributed denial-of-service (DDoS), eavesdropping, impersonation, replay, modification, spoofing, and ARP and DNS attacks. Be able to supply effective countermeasures for each.

Written Lab

1. Describe the differences between transport mode and tunnel mode of VPNs.
2. Discuss the benefits of NAT.
3. What are the main differences between circuit switching and packet switching?
4. What are some security issues with email and options for safeguarding against them?
5. What are the private IP addresses, APIPA addresses, and loopback addresses?
6. Name at least six facts about VLANs.

Review Questions

1. Among the many aspects of a security solution, the most important is whether it addresses a specific need (i.e., a threat) for your assets. But there are many other aspects of security you should consider as well. A significant benefit of a security control is when it goes unnoticed by users. What is this called?

   A. Invisibility

   B. Transparency

C. Diversion

D. Hiding in plain sight

2. Extensible Authentication Protocol (EAP) is one of the three authentication options provided by Point-to-Point Protocol (PPP). EAP allows customized authentication security solutions. Which of the following are examples of actual EAP methods? (Choose all that apply.)

   A. LEAP

   B. EAP-VPN

   C. PEAP

   D. EAP-SIM

   E. EAP-FAST

   F. EAP-MBL

   G. EAP-MD5

   H. VEAP

   I. EAP-POTP

   J. EAP-TLS

   K. EAP-TTLS

3. In addition to maintaining an updated system and controlling physical access, which of the following is the most effective countermeasure against PBX fraud and abuse?

   A. Encrypting communications

   B. Changing default passwords

   C. Using transmission logs

   D. Taping and archiving all conversations

4. A phreaker has been apprehended who had been exploiting the technology deployed in your office building. Several handcrafted tools and electronics were taken in as evidence that the phreaker had in their possession when they were arrested. What was this

adversary likely focusing on with their attempts to compromise the organization?

A. Accounting

B. NAT

C. PBX

D. Wi-Fi

5. Multimedia collaboration is the use of various multimedia-supporting communication solutions to enhance distance collaboration (people working on a project together remotely). Often, collaboration allows workers to work simultaneously as well as across different time frames. Which of the following are important security mechanisms to impose on multimedia collaboration tools? (Choose all that apply.)

   A. Encryption of communications

   B. Multifactor authentication

   C. Customization of avatars and filters

   D. Logging of events and activities

6. Michael is configuring a new web server to offer instruction manuals and specification sheets to customers. The web server has been positioned in the screened subnet and assigned an IP address of 172.31.201.17, and the public side of the company's split-DNS has associated the documents.myexamplecompany.com domain name with the assigned IP. After verifying that the website is accessible from his management station (which accesses the screened subnet via a jumpbox) as well as from several worker desktop systems, he declares the project completed and heads home. A few hours later, Michael thinks of a few additional modifications to perform to improve site navigation. However, when he attempts to connect to the new website using the FQDN, he receives a connection error stating that the site cannot be reached. What is the reason for this issue?

   A. The jumpbox was not rebooted.

B. Split-DNS does not support Internet domain name resolution.

C. The browser is not compatible with the site's coding.

D. A private IP address from RFC 1918 is assigned to the web server.

7. Mark is configuring the remote access server to receive inbound connections from remote workers. He is following a configuration checklist to ensure that the telecommuting links are compliant with company security policy. What authentication protocol offers no encryption or protection for logon credentials?

   A. PAP

   B. CHAP

   C. EAP

   D. RADIUS

8. Users have reported data loss and the inability to maintain connections throughout the workday. You suspect that something about the network structure has changed to cause this QoS reduction. Which of the following are aspects of networking you need to investigate to track down the issue? (Choose all that apply.)

   A. Bandwidth

   B. System uptime

   C. Latency

   D. Jitter

   E. Application Layer protocol

   F. Packet loss

   G. Interference

   H. Throughput

   I. OS versions

   J. Signal-to-noise ratio

9. While evaluating network traffic, you discover several addresses that you are not familiar with. Several of the addresses are in the range of addresses assigned to internal network segments. Which of the following IP addresses are private IPv4 addresses as defined by RFC 1918? (Choose all that apply.)

    A. 10.0.0.18

    B. 169.254.1:.119

    C. 172.31.8.204

    D. 192.168.6.43

10. The CISO has requested a report on the potential communication partners throughout the company. There is a plan to implement VPNs between all network segments in order to improve security against eavesdropping and data manipulation. Which of the following cannot be linked over a VPN?

    A. Two distant Internet-connected LANs

    B. Two systems on the same LAN

    C. A system connected to the Internet and a LAN connected to the Internet

    D. Two systems without an intermediary network connection

11. What networking device can be used to create digital virtual network segments that can be altered as needed by adjusting the settings internal to the device?

    A. Router

    B. Switch

    C. Proxy

    D. Firewall

12. The CISO is concerned that the use of subnets as the only form of network segments is limiting growth and flexibility of the network. They are considering the implementation of switches to support VLANs but aren't sure VLANs are the best option. Which of the following is not a benefit of VLANs?

A. Traffic isolation

B. Data/traffic encryption

C. Traffic management

D. Reduced vulnerability to sniffers

13. The CISO has tasked you to design and implement an IT port security strategy. While researching the options, you realize there are several potential concepts that are labeled as port security. You prepare a report to present options to the CISO. Which of the following are port security concepts you should include on this report? (Choose all that apply.)

    A. Shipping container storage

    B. NAC

    C. Transport Layer

    D. RJ-45 jacks

14. _____ is the oversight and management of the efficiency and performance of network communications. Items to measure include throughput rate, bit rate, packet loss, latency, jitter, transmission delay, and availability.

    A. VPN

    B. QoS

    C. SDN

    D. Sniffing

15. You are configuring a VPN to provide secure communications between systems. You want to minimize the information left in plaintext by the encryption mechanism of the chosen solution. Which IPSec mode provides for encryption of complete packets, including header information?

    A. Transport

    B. Encapsulating Security Payload

    C. Authentication Header

    D. Tunnel

16. Internet Protocol Security (IPSec) is a standard of IP security extensions used as an add-on for IPv4 and integrated into IPv6. What IPSec component provides assurances of message integrity and identity verification?

    A. Authentication Header

    B. Encapsulating Security Payload

    C. IP Payload Compression protocol

    D. Internet Key Exchange

17. When you're designing a security system for Internet-delivered email, which of the following is least important?

    A. Nonrepudiation

    B. Data remanent destruction

    C. Message integrity

    D. Access restriction

18. You have been tasked with crafting the organization's email retention policy. Which of the following is typically not an element that must be discussed with end users in regard to email retention policies?

    A. Privacy

    B. Auditor review

    C. Length of retainer

    D. Backup method

19. Modern networks are built on multilayer protocols, such as TCP/IP. This provides for flexibility and resiliency in complex network structures. All of the following are implications of multilayer protocols except which one?

    A. VLAN hopping

    B. Multiple encapsulation

    C. Filter evasion using tunneling

    D. Static IP addressing

20. Which of the following is a type of connection that can be described as a logical circuit that always exists and is waiting for the customer to send data?

A. SDN

B. PVC

C. VPN

D. SVC